ZyWALL 50

Internet Security Gateway

User's Guide

Version 3.50

November 2001

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Copyright

Copyright © 2001 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.
Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective operation and safety requirements. The Industry Canada label does not guarantee that the equipment will operate to a user's satisfaction.
Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.
Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

Declaration of Conformity

We, the Manufacturer/Importer,

ZyXEL Communications Corp.
No. 6, Innovation Rd. II,
Science-Based Industrial Park,
Hsinchu, Taiwan, 300 R.O.C

declare that the product

ZyWALL 50

is in conformity with

(reference to the specification under which conformity is declared)

Standard	*Standard Item*	Version
• EN 55022	Radio disturbance characteristics — Limits and method of measurement.	1994
• EN 61000-3-2	Disturbance in supply system caused by household appliances and similar electrical equipment “Harmonics”.	1995
• EN 61000-3-3	Disturbance in supply system caused by household appliances and similar electrical equipment “Voltage fluctuations”.	1995
• EN 61000-4-2	Electrostatic discharge immunity test — Basic EMC Publication	1995
• EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test	1996
• EN 61000-4-4	Electrical fast transient / burst immunity test - Basic EMC Publication	1995
• EN 61000-4-5	Surge immunity test	1995
• EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields	1996
• EN 61000-4-8		1993
• EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	1994

Certifications

Refer to the product page at www.zyxel.com.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Don’t forget to register your ZyXEL product (fast, easy online registration at www.zyxel.com) for free future product updates and information.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Information in **Menu 24.2.1 – System Information**.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw support@europe.zyxel.com sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan 300, R.O.C.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
AUSTRIA	support@zyxel.at sales@zyxel.at	+43-1-4948677-0 +43-1-4948678	www.zyxel.at ftp.zyxel.at	ZyXEL Communications Services GmbH. Thaliastrasse 125a/2/2/4 A-1160 Vienna, Austria
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A4 D-52146 Wuerselen, Germany
MALAYSIA	support@zyxel.com.my sales@zyxel.com.my	+603-795-44-688 +603-795-34-407	www.zyxel.com.my	Lot B2-06, PJ Industrial Park, Section 13, Jalan Kemajuan, 46200 Petaling Jaya Selangor Darul Ehasn, Malaysia

Table of Contents

Copyright ..... **ii**

Federal Communications Commission (FCC) Interference Statement ..... **iii**

Information for Canadian Users ..... **iv**

ZyXEL Limited Warranty ..... **vi**

Customer Support ..... **vii**

List of Figures ..... **xix**

List Of Tables ..... **xxvi**

Preface ..... **xxxi**

GETTING STARTED ..... **I**

Chapter 1 Getting to Know Your ZyWALL **1-1**

1.1 The ZyWALL 50 Internet Security Gateway 1-1

1.2 Features of The ZyWALL 50 1-1

1.3 Applications for the ZyWALL 50 1-4

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem 1-4

1.3.2 VPN Application 1-5

Chapter 2 Hardware Installation **2-1**

2.1 Front Panel LEDs and Back Panel Ports 2-1

2.1.1 Front Panel LEDs 2-1

2.2 ZyWALL 50 Rear Panel and Connections 2-2

2.3 Additional Installation Requirements 2-5

Chapter 3 Initial Setup **3-1**

3.1 Turning On Your ZyWALL 3-1

3.1.1 Initial Screen 3-1
3.1.2 Entering the Password 3-1
3.2 Navigating the SMT Interface 3-2
3.2.1 Main Menu 3-3
3.2.2 System Management Terminal Interface Summary 3-3
3.2.3 SMT Menus at a Glance 3-5
3.3 Changing the System Password 3-7
3.4 Resetting the ZyWALL 3-8
3.4.1 Methods of Restoring Factory-Defaults 3-8
3.4.2 Procedure To Use The Reset Button 3-9
Chapter 4 General And WAN Setup 4-1
4.1 System Name 4-1
4.2 Dynamic DNS 4-1
4.3 WAN Setup 4-3
Chapter 5 LAN Setup 5-1
5.1 Introduction 5-1
5.2 LAN Port Filter Setup 5-1
5.3 TCP/IP and DHCP for LAN 5-1
5.3.1 Factory LAN Defaults 5-2
5.3.2 DHCP Configuration 5-2
5.3.3 IP Address and Subnet Mask 5-2
5.3.4 Private IP Addresses 5-3
5.3.5 RIP Setup 5-4
5.3.6 IP Multicast 5-4
5.3.7 IP Alias 5-5
5.4 TCP/IP and DHCP Ethernet Setup Menu 5-5
5.4.1 IP Alias Setup 5-7

Chapter 6 Internet Access 6-1

6.1 Internet Access Setup 6-1

6.1.1 Ethernet Encapsulation 6-1

6.1.2 PPTP Encapsulation 6-2

6.1.3 Configuring the PPTP Client 6-3

6.1.4 PPPoE Encapsulation 6-4

6.2 Basic Setup Complete 6-5

ADVANCED APPLICATIONS II

Chapter 4 Remote Node Setup 4-1

4.1 Remote Node Profile 4-1

4.1.1 Ethernet Encapsulation 4-1

4.1.2 PPPoE Encapsulation 4-3

4.1.3 PPTP Encapsulation 4-5

4.2 Editing TCP/IP Options (with Ethernet Encapsulation) 4-7

4.2.1 Editing TCP/IP Options (with PPTP Encapsulation) 4-8

4.2.2 Editing TCP/IP Options (with PPPoE Encapsulation) 4-10

4.3 Remote Node Filter 4-10

Chapter 5 IP Static Route Setup 5-1

5.1 IP Static Route Setup 5-2

Chapter 6 Network Address Translation (NAT) 6-1

6.1 Introduction 6-1

6.1.1 NAT Definitions 6-1

6.1.2 What NAT Does 6-2

6.1.3 How NAT Works 6-2

6.1.4 NAT Application 6-3

6.1.5 NAT Mapping Types 6-4

6.2 Using NAT 6-6

6.2.1 SUA (Single User Account) Versus NAT 6-6
6.2.2 Applying NAT 6-6
6.3 NAT Setup 6-8
6.3.1 Address Mapping Sets 6-8
6.4 NAT Server Sets – Port Forwarding 6-13
6.4.1 Configuring a Server behind NAT 6-14
6.5 General NAT Examples 6-16
6.5.1 Internet Access Only 6-16
6.5.2 Example 2: Internet Access with an Inside Server 6-17
6.5.3 Example 3: Multiple Public IP Addresses With Inside Servers 6-18
6.5.4 Example 4: NAT Unfriendly Application Programs 6-22
FIREWALL AND CONTENT FILTERS III
Chapter 7 Firewalls 7-1
7.1 What Is a Firewall? 7-1
7.2 Types of Firewalls 7-1
7.2.1 Packet Filtering Firewalls 7-1
7.2.2 Application-level Firewalls 7-1
7.2.3 Stateful Inspection Firewalls 7-2
7.3 Introduction to ZyXEL's Firewall 7-2
7.4 Denial of Service 7-3
7.4.1 Basics 7-3
7.4.2 Types of DoS Attacks 7-4
7.5 Stateful Inspection 7-7
7.5.1 Stateful Inspection Process 7-8
7.5.2 Stateful Inspection and the ZyWALL 7-9
7.5.3 TCP Security 7-10
7.5.4 UDP/ICMP Security 7-10
7.5.5 Upper Layer Protocols 7-11

7.6 Guidelines For Enhancing Security With Your Firewall 7-11
7.6.1 Security In General 7-12
7.7 Packet Filtering Vs Firewall 7-12
7.7.1 Packet Filtering: 7-13
7.7.2 Firewall 7-13
Chapter 8 Introducing the ZyWALL Firewall 8-1
8.1 Remote Management and the Firewall 8-1
8.2 Access Methods 8-1
8.3 Using ZyWALL SMT Menus 8-1
8.3.1 Activating the Firewall 8-1
8.3.2 Viewing the Firewall Log 8-2
Chapter 9 Using the ZyWALL Web Configurator 9-1
9.1 Web Configurator Login and Main Menu Screens 9-1
9.2 Enabling the Firewall 9-3
9.3 E-mail 9-3
9.3.1 Alerts 9-3
9.3.2 Logs 9-4
9.3.3 SMTP Error Messages 9-6
9.3.4 Example E-mail Log 9-6
9.4 Attack Alert 9-7
9.4.1 Threshold Values 9-7
9.4.2 Half-Open Sessions 9-8
Chapter 10 Creating Custom Rules 10-1
10.1 Rules Overview 10-1
10.2 Rule Logic Overview 10-1
10.2.1 Rule Checklist 10-1
10.2.2 Security Ramifications 10-2

10.2.3 Key Fields For Configuring Rules 10-2
10.3 Connection Direction 10-3
10.3.1 LAN to WAN Rules 10-3
10.3.2 WAN to LAN Rules 10-4
10.4 Rule Summary 10-4
10.5 Predefined Services 10-7
10.5.1 Creating/Editing Firewall Rules 10-10
10.5.2 Source and Destination Addresses 10-11
10.6 Timeout 10-13
10.6.1 Factors Influencing Choices for Timeout Values 10-13
Chapter 11 Custom Ports 11-1
11.1 Introduction 11-1
11.2 Creating/Editing A Custom Port 11-3
Chapter 12 Logs 12-1
12.1 Log Screen 12-1
Chapter 13 Example Firewall Rules 13-1
13.1 Examples 13-1
13.1.1 Example 1: Firewall Rule To Allow Web Service From The Internet 13-1
13.1.2 Example 2: Small Office With Mail, FTP and Web Servers 13-6
13.1.3 Example 3: DHCP Negotiation and Syslog Connection from the Internet 13-12
Chapter 14 Content Filtering 14-1
14.1 Categories 14-1
14.1.1 Restrict Web Features 14-1
14.1.2 Filter List 14-1
14.1.3 Days and Times 14-1
14.2 Update List 14-1

14.3 Exempt Computers 14-1
14.4 Customizing 14-2
14.5 Keywords 14-2
14.6 Log Records 14-2
ADVANCED MANAGEMENT IV
Chapter 15 Filter Configuration 15-1
15.1 About Filtering 15-1
15.1.1 The Filter Structure of the ZyWALL 15-2
15.2 Configuring a Filter Set 15-4
15.2.1 Filter Rules Summary Menu 15-6
15.2.2 Configuring a Filter Rule 15-7
15.2.3 TCP/IP Filter Rule 15-7
15.2.4 Generic Filter Rule 15-12
15.3 Example Filter 15-14
15.4 Filter Types and NAT 15-17
15.5 Firewall 15-17
15.6 Applying a Filter and Factory Defaults 15-18
15.6.1 LAN traffic 15-18
15.6.2 Remote Node Filters 15-18
Chapter 16 SNMP Configuration 16-1
16.1 About SNMP 16-1
16.2 Supported MIBs 16-3
16.3 Configuring SNMP 16-3
16.4 SNMP Traps 16-4
Chapter 17 System Information & Diagnosis 17-1

17.1 System Status 17-1
17.2 System Information and Console Port Speed 17-3
17.2.1 System Information 17-4
17.2.2 Console Port Speed 17-5
17.3 Log and Trace 17-5
17.3.1 Viewing Error Log 17-5
17.3.2 UNIX Syslog 17-7
17.3.3 Call-Triggering Packet 17-10
17.4 Diagnostic 17-11
17.4.1 WAN DHCP 17-12
Chapter 18 Firmware and Configuration Maintenance 18-1
18.1 Filename Conventions 18-1
18.2 Backup Configuration 18-2
18.2.1 Backup Configuration 18-2
18.2.2 Using the FTP Command from the Command Line 18-3
18.2.3 Example of FTP Commands from the Command Line 18-3
18.2.4 GUI-Based FTP Clients 18-4
18.2.5 TFTP and FTP over WAN Will Not Work When 18-4
18.2.6 Backup Configuration Using TFTP 18-5
18.2.7 TFTP Command Example 18-5
18.2.8 GUI-Based TFTP Clients 18-6
18.2.9 Backup Via Console Port 18-6
18.3 Restore Configuration 18-7
18.3.1 Restore Using FTP or TFTP 18-8
18.3.2 Procedure To Restore Using FTP 18-8
18.3.3 Restore Using FTP Session Example 18-9
18.3.4 Restore Via Console Port 18-9
18.4 Uploading Firmware and Configuration Files 18-10
18.4.1 Firmware File Upload 18-11

18.4.2 Configuration File Upload 18-11
18.4.3 FTP File Upload Command from the Command Line Example 18-12
18.4.4 FTP Session Example of Firmware File Upload 18-13
18.4.5 TFTP File Upload 18-13
18.4.6 TFTP Upload Command Example 18-14
18.4.7 Uploading Via Console Port 18-14
18.4.8 Uploading a Firmware File Via Console Port 18-14
18.4.9 Example Xmodem Firmware Upload Using HyperTerminal 18-15
18.4.10 Uploading a Configuration File Via Console Port 18-16
18.4.11 Example Xmodem Configuration Upload Using HyperTerminal 18-16

Chapter 19 System Maintenance & Information 19-1

19.1 Command Interpreter Mode 19-1
19.2 Call Control Support 19-2
19.2.1 Budget Management 19-2
19.2.2 Call History 19-4
19.3 Time and Date Setting 19-5
19.3.1 Resetting the Time 19-7

Chapter 20 Remote Management 20-1

20.1 Telnet 20-1
20.2 FTP 20-1
20.3 Web 20-2
20.4 Remote Management 20-2
20.4.1 Remote Management Limitations 20-3
20.5 Remote Management and NAT 20-4
20.6 System Timeout 20-4

CALL SCHEDULING AND VPN/IPSEC V

Chapter 21 Call Scheduling 21-1

21.1 Introduction 21-1

Chapter 22 Introduction to IPSec 22-1

22.1 Introduction 22-1
22.1.1 VPN 22-1
22.1.2 IPSec 22-1
22.1.3 Security Association 22-1
22.1.4 Other Terminology 22-1
22.1.5 VPN Applications 22-2
22.2 IPSec Architecture 22-3
22.2.1 IPSec Algorithms 22-4
22.2.2 Key Management 22-4
22.3 Encapsulation 22-5
22.3.1 Transport Mode 22-5
22.3.2 Tunnel Mode 22-5
22.4 IPSec and NAT 22-5

Chapter 23 VPN/IPSec Setup 23-1

23.1 VPN/IPSec Setup 23-1
23.2 IPSec Algorithms 23-2
23.2.1 AH (Authentication Header) Protocol 23-2
23.2.2 ESP (Encapsulating Security Payload) Protocol 23-2
23.3 IPSec Summary 23-3
23.3.1 IPSec Setup 23-7
23.4 IKE Setup 23-10
23.4.1 IKE Phases 23-10
23.4.2 Negotiation Mode 23-11
23.4.3 Pre-Shared Key 23-12
23.4.4 Diffie-Hellman (DH) Key Groups 23-12
23.4.5 Perfect Forward Secrecy (PFS) 23-12

23.5 Manual Setup 23-15
23.5.1 Active Protocol 23-15
23.5.2 Security Parameter Index (SPI) 23-15
Chapter 24 SA Monitor 24-1
1.1. Introduction 24-1
Chapter 25 IPSec Log 25-1
TROUBLESHOOTING, APPENDICES AND INDEX VI
Chapter 26 Troubleshooting 26-1
26.1 Problems Starting Up the ZyWALL 26-1
26.2 Problems with the LAN Interface 26-2
26.3 Problems with the WAN interface 26-2
26.4 Problems with Internet Access 26-3
26.5 Problems with the Password 26-3
26.6 Problems with Remote Management 26-3
Appendix A The Big Picture ..... A
Appendix B PPPoE C
Appendix C PPTP ..... E
Appendix D Hardware Specifications ..... H
Appendix E Important Safety Instructions I
Appendix F Boot Commands ..... K
Appendix G Firewall CLI Commands ..... M
Appendix H Power Adapter Specifications ..... R
Index ..... U

List of Figures

Figure 1-1 Secure Internet Access via Cable 1-4
Figure 1-2 Secure Internet Access via DSL 1-4
Figure 1-3 VPN Application 1-5
Figure 2-1 Front Panel 2-1
Figure 2-2 ZyWALL 50 Rear Panel and Connections 2-3
Figure 3-1 Initial Screen 3-1
Figure 3-2 Password Screen 3-2
Figure 3-3 ZyWALL Main Menu 3-3
Figure 3-4 Getting Started and Advanced Applications SMT Menus 3-5
Figure 3-5 Advanced Management SMT Menus 3-6
Figure 3-6 IPSec VPN Configuration SMT Menus 3-7
Figure 3-7 Menu 23 — System Password 3-7
Figure 4-1 Configure Dynamic DNS 4-2
Figure 4-2 Menu 2 — WAN Setup 4-4
Figure 5-1 Menu 3 — LAN Setup 5-1
Figure 5-2 Menu 3.1 — LAN Port Filter Setup 5-1
Figure 5-3 Physical Network 5-5
Figure 5-4 Partitioned Logical Networks 5-5
Figure 5-5 Menu 3 — TCP/IP and DHCP Setup 5-5
Figure 5-6 Menu 3.2 — TCP/IP and DHCP Ethernet Setup 5-6
Figure 5-7 Menu 3.2.1 — IP Alias Setup 5-8
Figure 6-1 Menu 4 — Internet Access Setup (Ethernet) 6-1
Figure 6-2 Internet Access Setup (PPTP) 6-3
Figure 6-3 Internet Access Setup (PPPoE) 6-4
Figure 4-1 Menu 11.1 — Remote Node Profile for Ethernet Encapsulation 4-2

Figure 4-2 Menu 11.1 — Remote Node Profile for PPPoE Encapsulation 4-4
Figure 4-3 Menu 11.1 — Remote Node Profile for PPTP Encapsulation 4-6
Figure 4-4 Menu 11.3 — Remote Node Network Layer Options 4-7
Figure 4-5 Menu 11.3 — Remote Node Network Layer Options 4-9
Figure 4-6 Menu 11.5 — Remote Node Filter (Ethernet Encapsulation) 4-11
Figure 4-7 Menu 11.5 — Remote Node Filter (PPPoE or PPTP Encapsulation) 4-11
Figure 5-1 Example of Static Routing Topology 5-1
Figure 5-2 Menu 12 — IP Static Route Setup 5-2
Figure 5-3 Menu 12. 1 — Edit IP Static Route 5-2
Figure 6-1 How NAT Works 6-3
Figure 6-2 NAT Application With IP Alias 6-4
Figure 6-3 Menu 4 — Applying NAT for Internet Access 6-6
Figure 6-4 Menu 11.3 — Applying NAT to the Remote Node 6-7
Figure 6-5 Menu 15 — NAT Setup 6-8
Figure 6-6 Menu 15.1 — Address Mapping Sets 6-8
Figure 6-7 Menu 15.1.255 — SUA Address Mapping Rules 6-9
Figure 6-8 Menu 15.1.1 — First Set 6-10
Figure 6-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set 6-12
Figure 6-10 Menu 15.2 — NAT Server Setup 6-15
Figure 6-11 Multiple Servers Behind NAT Example 6-15
Figure 6-12 NAT Example 1 6-16
Figure 6-13 Menu 4 — Internet Access & NAT Example 6-16
Figure 6-14 NAT Example 2 6-17
Figure 6-15 Menu 15.2 — Specifying an Inside Server 6-18
Figure 6-16 NAT Example 3 6-19
Figure 6-17 Example 3: Menu 11.3 6-20
Figure 6-18 Example 3: Menu 15.1.1.1 6-20

Figure 6-19 Example 3: Final Menu 15.1.1 6-21
Figure 6-20 Example 3: Menu 15.2 6-21
Figure 6-21 NAT Example 4 6-22
Figure 6-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule 6-23
Figure 6-23 Example 4: Menu 15.1.1 — Address Mapping Rules 6-23
Figure 7-1 ZyWALL Firewall Application 7-3
Figure 7-2 Three-Way Handshake 7-5
Figure 7-3 SYN Flood 7-5
Figure 7-4 Smurf Attack 7-6
Figure 7-5 Stateful Inspection 7-8
Figure 8-1 Menu 21 — Filter and Firewall Setup 8-1
Figure 8-2 Menu 21.2 — Firewall Setup 8-2
Figure 8-3 Example Firewall Log 8-2
Figure 9-1 Main Menu 9-2
Figure 9-2 Enabling the Firewall 9-3
Figure 9-3 E-mail Screen 9-4
Figure 9-4 E-mail Log 9-7
Figure 9-5 Attack Alert 9-9
Figure 10-1 LAN to WAN Traffic 10-3
Figure 10-2 WAN to LAN Traffic 10-4
Figure 10-3 Firewall Rules Summary — First Screen 10-5
Figure 10-4 Creating/Editing A Firewall Rule 10-10
Figure 10-5 Adding/Editing Source and Destination Addresses 10-12
Figure 10-6 Timeout Screen 10-14
Figure 11-1 Custom Ports 11-1
Figure 11-2 Creating/Editing A Custom Port 11-3
Figure 12-1 Log Screen 12-1

Figure 13-1 Activate the Firewall 13-2
Figure 13-2 Example 1: E-Mail Screen 13-3
Figure 13-3 Example 1: Configuring a Rule 13-4
Figure 13-4 Example 1: Destination Address for Traffic Originating from the Internet 13-5
Figure 13-5 Example 1: Rule Summary Screen 13-6
Figure 13-6 Send Alerts When Attacked 13-7
Figure 13-7 Configuring A POP Custom Port 13-8
Figure 13-8 Example 2: Local Network Rule 1 Configuration 13-9
Figure 13-9 Example 2: Local Network Rule Summary 13-10
Figure 13-10 Example: Internet to Local Network Rule Summary 13-11
Figure 13-11 Custom Port for Syslog 13-12
Figure 13-12 Syslog Rule Configuration 13-13
Figure 13-13 Example 3: Rule Summary 13-14
Figure 15-1 Outgoing Packet Filtering Process 15-2
Figure 15-2 Filter Rule Process 15-3
Figure 15-4 Menu 21 — Filter and Firewall Setup 15-4
Figure 15-5 Menu 21.1 — Filter Set Configuration 15-4
Figure 15-6 NetBIOS_WAN Filter Rules Summary 15-5
Figure 15-7 NetBIOS _LAN Filter Rules Summary 15-5
Figure 15-8 Menu 21.1.1.1 — TCP/IP Filter Rule 15-8
Figure 15-9 Executing an IP Filter 15-11
Figure 15-10 Menu 21.4.1.1 — Generic Filter Rule 15-12
Figure 15-11 Telnet Filter Example 15-14
Figure 15-12 Example Filter — Menu 21.1.3.1 15-15
Figure 15-13 Example Filter Rules Summary — Menu 21.1.3 15-16
Figure 15-14 Protocol and Device Filter Sets 15-17
Figure 15-15 Filtering LAN Traffic 15-18

Figure 15-16 Filtering Remote Node Traffic 15-19
Figure 16-1 SNMP Management Model 16-2
Figure 16-2 Menu 22 — SNMP Configuration 16-4
Figure 17-1 Menu 24 — System Maintenance 17-1
Figure 17-2 Menu 24.1 — System Maintenance — Status 17-2
Figure 17-3 Menu 24.2 — System Information and Console Port Speed 17-4
Figure 17-4 Menu 24.2.1 — System Maintenance — Information 17-4
Figure 17-5 Menu 24.2.2 — System Maintenance — Change Console Port Speed 17-5
Figure 17-6 Menu 24.3 — System Maintenance — Log and Trace 17-6
Figure 17-7 Examples of Error and Information Messages 17-6
Figure 17-8 Menu 24.3.2 — System Maintenance — UNIX Syslog 17-7
Figure 17-9 Call-Triggering Packet Example 17-11
Figure 17-10 Menu 24.4 — System Maintenance — Diagnostic 17-12
Figure 17-11 WAN & LAN DHCP 17-13
Figure 18-1 Telnet in Menu 24.5 18-3
Figure 18-2 FTP Session Example 18-4
Figure 18-3 System Maintenance — Backup Configuration 18-6
Figure 18-4 System Maintenance — Starting Xmodem Download Screen 18-7
Figure 18-5 Backup Configuration Example 18-7
Figure 18-6 Successful Backup Confirmation Screen 18-7
Figure 18-7 Telnet into Menu 24.6 18-8
Figure 18-8 Restore Using FTP or TFTP Session Example 18-9
Figure 18-9 System Maintenance — Restore Configuration 18-9
Figure 18-10 System Maintenance — Starting Xmodem Download Screen 18-10
Figure 18-11 Restore Configuration Example 18-10
Figure 18-12 Successful Restoration Confirmation Screen 18-10
Figure 18-13 Telnet Into Menu 24.7.1 — Upload System Firmware 18-11

Figure 18-14 Telnet Into Menu 24.7.2 — System Maintenance 18-12
Figure 18-15 FTP Session Example of Firmware File Upload 18-13
Figure 18-16 Menu 24.7.1 as seen using the Console Port 18-15
Figure 18-17 Example Xmodem Upload 18-15
Figure 18-18 Menu 24.7.2 as seen using the Console Port 18-16
Figure 18-19 Example Xmodem Upload 18-17
Figure 19-1 Command Mode in Menu 24 19-1
Figure 19-2 Valid Commands 19-2
Figure 19-3 Call Control 19-2
Figure 19-4 Budget Management 19-3
Figure 19-5 Call History 19-4
Figure 19-6 Menu 24 — System Maintenance 19-5
Figure 19-7 Menu 24.10 System Maintenance — Time and Date Setting 19-6
Figure 20-1 Telnet Configuration on a TCP/IP Network 20-1
Figure 20-2 Menu 24.11 – Remote Management Control 20-2
Figure 21-1 Menu 26 - Schedule Setup 21-1
Figure 21-2 Schedule Set Setup 21-2
Figure 21-3 Applying Schedule Set(s) to a Remote Node (PPPoE) 21-4
Figure 21-4 Applying Schedule Set(s) to a Remote Node (PPTP) 21-4
Figure 22-1 Encryption and Decryption 22-2
Figure 22-2 VPN Application 22-3
Figure 22-3 IPSec Architecture 22-4
Figure 22-4 Transport and Tunnel Mode IPSec Encapsulation 22-5
Figure 23-1 VPN SMT Menu Tree 23-1
Figure 23-2 Menu 27 — VPN/IPSec Setup 23-2
Figure 23-3 IPSec Summary Fields 23-3
Figure 23-4 Telecommuter’s ZyWALL Configuration 23-4

Figure 23-5 HQ ZyWALL Configuration 23-5
Figure 23-6 Menu 27.1 — IPSec Summary 23-5
Figure 23-7 Menu 27.1.1 — IPSec Setup 23-8
Figure 23-8 Two Phases to set up the IPSec SA 23-11
Figure 23-9 Menu 27.1.1.1 — IKE Setup 23-13
Figure 23-10 Menu 27.1.1.2 — Manual Setup 23-16
Figure 24-1 Menu 27.2 — SA Monitor 24-1
Figure 25-1 Example VPN Initiator IPSec Log 25-1
Figure 25-2 Example VPN Responder IPSec Log 25-1

List Of Tables

Table 2-1 LED Descriptions 2-1
Table 3-1 Main Menu Commands 3-2
Table 3-2 Main Menu Summary 3-3
Table 4-1 Configure Dynamic DNS Menu Fields 4-2
Table 4-2 WAN Setup Menu Fields 4-4
Table 5-1 Example of Network Properties for LAN Servers with Fixed IP Addresses 5-2
Table 5-2 Private IP Address Ranges 5-3
Table 5-3 DHCP Ethernet Setup Menu Fields 5-6
Table 5-4 LAN TCP/IP Setup Menu Fields 5-7
Table 5-5 IP Alias Setup Menu Fields 5-8
Table 6-1 Internet Access Setup Menu Fields 6-1
Table 6-2 New Fields in Menu 4 (PPTP) screen 6-3
Table 6-3 New Fields in Menu 4 (PPPoE) screen 6-4
Table 4-1 Fields in Menu 11.1 4-2
Table 4-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific) 4-5
Table 4-3 Fields in Menu 11.1 (PPTP Encapsulation) 4-6
Table 4-4 Remote Node Network Layer Options Menu Fields 4-7
Table 4-5 Remote Node Network Layer Options Menu Fields 4-9
Table 5-1 IP Static Route Menu Fields 5-3
Table 6-1 NAT Definitions 6-1
Table 6-2 NAT Mapping Types 6-5

Table 6-3 Applying NAT in Menus 4 & 11.3 6-7
Table 6-4 SUA Address Mapping Rules 6-9
Table 6-5 Fields in Menu 15.1.1 6-11
Table 6-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set 6-12
Table 6-7 Services & Port Numbers 6-13
Table 7-1 Common IP Ports 7-4
Table 7-2 ICMP Commands That Trigger Alerts 7-6
Table 7-3 Legal NetBIOS Commands 7-7
Table 7-4 Legal SMTP Commands 7-7
Table 8-1 View Firewall Log 8-2
Table 9-1 E-mail 9-5
Table 9-2 SMTP Error Messages 9-6
Table 9-3 Attack Alert 9-9
Table 10-1 Firewall Rules Summary — First Screen 10-5
Table 10-2 Predefined Services 10-7
Table 10-3 Creating/Editing A Firewall Rule 10-10
Table 10-4 Adding/Editing Source and Destination Addresses 10-13
Table 10-5 Timeout Menu 10-15
Table 11-1 Custom Ports 11-2
Table 11-2 Creating/Editing A Custom Port 11-4
Table 12-1 Log Screen 12-2
Table 15-1 Abbreviations Used in the Filter Rules Summary Menu 15-6
Table 15-2 Rule Abbreviations Used 15-6

Table 15-3 TCP/IP Filter Rule Menu Fields 15-8
Table 15-4 Generic Filter Rule Menu Fields 15-13
Table 16-1 General SNMP Commands 16-3
Table 16-2 SNMP Configuration Menu Fields 16-4
Table 16-3 SNMP Traps 16-5
Table 17-1 System Maintenance — Status Menu Fields 17-2
Table 17-2 Fields in System Maintenance — Information 17-4
Table 17-3 System Maintenance Menu Syslog Parameters 17-7
Table 17-4 System Maintenance Menu Diagnostic 17-13
Table 18-1 Filename Conventions 18-2
Table 18-2 General Commands for GUI-Based FTP Clients 18-4
Table 18-3 General Commands for GUI-Based TFTP Clients 18-6
Table 19-1 Budget Management 19-3
Table 19-2 Call History Fields 19-4
Table 19-3 Time and Date Setting Fields 19-6
Table 20-1 Menu 24.11 – Remote Management Control 20-3
Table 21-1 Schedule Set Setup Fields 21-2
Table 22-1 VPN and NAT 22-6
Table 23-1 AH and ESP 23-3
Table 23-2 Telecommuter and HQ Configuration Example 23-4
Table 23-3 Menu 27.1 — IPSec Summary 23-6
Table 23-4 Menu 27.1.1 — IPSec Setup 23-8
Table 23-5 Menu 27.1.1.1 — IKE Setup 23-13

Table 23-6 Active Protocol — Encapsulation and Security Protocol 23-15
Table 23-7 Menu 27.1.1.2 — Manual Setup 23-16
Table 24-1 Menu 27.2 — SA Monitor 24-1
Table 25-1 Sample IKE Key Exchange Logs 25-2
Table 25-2 Sample IPSec Logs During Packet Transmission 25-3
Table 25-3 RFC-2408 ISAKMP Payload Types 25-4
Table 26-1 Troubleshooting the Start-Up of your ZyWALL 26-1
Table 26-2 Troubleshooting the LAN Interface 26-2
Table 26-3 Troubleshooting the WAN interface 26-2
Table 26-4 Troubleshooting Internet Access 26-3
Table 26-5 Troubleshooting the Password 26-3
Table 26-6 Troubleshooting Remote Management 26-4

Preface

About Your ZyWALL

Congratulations on your purchase of the ZyWALL 50 Internet Security Gateway.

Don't forget to register your ZyWALL (fast, easy online registration at www.zyxel.com) for free future product updates and information.

The ZyWALL 50 is a dual Ethernet Internet Security Gateway integrated with robust firewall solutions and network management features that allows access to the Internet via cable/ADSL modem or Internet router. It is designed for:

- Home offices and small businesses with cable, xDSL and wireless modem via Ethernet port as Internet access media.
- Multiple office/department connections via access devices.
- E-commerce/EDI applications.

The ZyWALL 50 features an ICSA certified firewall, IPSec VPN capability (allowing up to 50 simultaneous secure connections), MultiNAT (for multiple IP address translation), web page content filtering and an embedded web server for easy configuration. See the next chapter for more details on these and other features.

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyWALLs' management settings and configure the firewall. There is an embedded web help (click the Help button) for the configurator as well as more comprehensive HTML help on the accompanying CD.
Most functions of the ZyWALL are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection.

You can configure most features of the ZyWALL 50 via SMT but we recommend you configure the firewall using the ZyWALL Web Configurator.

About This User's Manual

This manual is designed to guide you through the SMT configuration of your ZyWALL 50 for its various applications. There is also HTML help for the embedded web configurator.

Related Documentation

- Supporting Disk
  More detailed information about the ZyWALL and examples of its use can be found in our included disk (as well as on the zyxel.com web site). This disk contains information on configuring your ZyWALL for Internet Access, a general FAQ, an advanced FAQ, Application Notes, Troubleshooting, a reference for CI Commands as well as bundled software.
- Quick Start Guide

Our Quick Start Guide is designed to help you get your ZyWALL up and running right away. It contains a detailed easy-to-follow connection diagram, ZyWALL default settings, handy checklists, information on setting up your network and information on configuring your ZyWALL for Internet access.

- Packing List Card
  Finally, you should have a Packing List Card, which lists all items that should have come with your ZyWALL.
- Glossary
  Please refer to www.zyxel.com for an online glossary of networking terms.
- ZyXEL Web Site
  The ZyXEL download library at www.zyxel.com contains additional support documentation.

Syntax Conventions

- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to make a selection from one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times** font. The choices of a menu item are in **Bold Arial** font. A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.
- For brevity's sake, we will use "e.g." as a shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.

The ZyWALL 50 may be referred to simply as the ZyWALL throughout this manual.

Part I:

Getting Started

This part is structured as a step-by-step guide to help you connect, install and setup your ZyWALL to operate on your network and access the Internet.

Chapter 1
Getting to Know Your ZyWALL

This chapter introduces the main features and applications of the ZyWALL.

1.1 The ZyWALL 50 Internet Security Gateway

The ZyWALL 50 is a dual Ethernet Internet security gateway integrated with a robust firewall and network management features designed for home offices and small businesses to access the Internet via cable/ADSL modem or Internet router.

By integrating NAT, firewall and VPN capability, ZyXEL's ZyWALL 50 provides not only ease of installation and Internet access, but also a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

The ZyWALL web configurator is a breeze to operate and totally independent of the operating system platform you use.

1.2 Features of The ZyWALL 50

The following are the main features of the ZyWALL 50.

Auto-negotiating 10/100Mbps Ethernet LAN

This auto-negotiation feature allows the ZyWALL to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

IPSec VPN Capability

Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The ZyWALL 50 VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products. The ZyWALL 50 supports up to 50 runtime SAs (Security Associations).

Firewall

The ZyWALL is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyWALL firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

You can configure most features of the ZyWALL 50 via SMT but we recommend you configure the firewall and Content Filters using the ZyWALL web configurator.

Content Filtering

The ZyWALL can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The ZyWALL can also block specific URLs by using the keyword feature.

Packet Filtering

The Packet Filtering mechanism blocks unwanted traffic from entering/leaving your network.

Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The ZyWALL supports one PPTP server connection at any given time.

Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS client to use this service.

IP Multicast

Deliver IP packets to a specific group of hosts (only) using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the ZyWALL supports both versions 1 and 2.

IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1).

Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of an Internet Protocol address used within one network to a different IP address known within another network.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyWALL has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 9X, Windows NT and other systems that support the DHCP client. The ZyWALL can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

Full Network Management

This feature allows you to access the SMT (System Management Terminal) through the console port or telnet connection.

RoadRunner Support

In addition to standard cable modem services, the ZyWALL supports Time Warner's RoadRunner Service.

Time and Date Setting

This new feature (Menu 24.10) allows you to get the current time and date from an external server when you power up your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs. If you do not choose a time service protocol that your timeserver will send when the ZyWALL powers up, you can enter the time manually but each time the system is booted, the time and date will be reset to 2000/01/0100:00:00.

Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.

Upgrade ZyWALL Firmware via LAN

The firmware of the ZyWALL 50 can be upgraded via the LAN.

Embedded FTP and TFTP Servers

The ZyWALL's embedded FTP and TFTP Servers enable fast firmware upgrades as well as configuration file backups and restoration.

1.3 Applications for the ZyWALL 50

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

A cable modem or xDSL modem can connect to the ZyWALL 50 for broadband Internet access via Ethernet port on the modem. It provides not only high speed Internet access, but secured internal network protection and management as well.

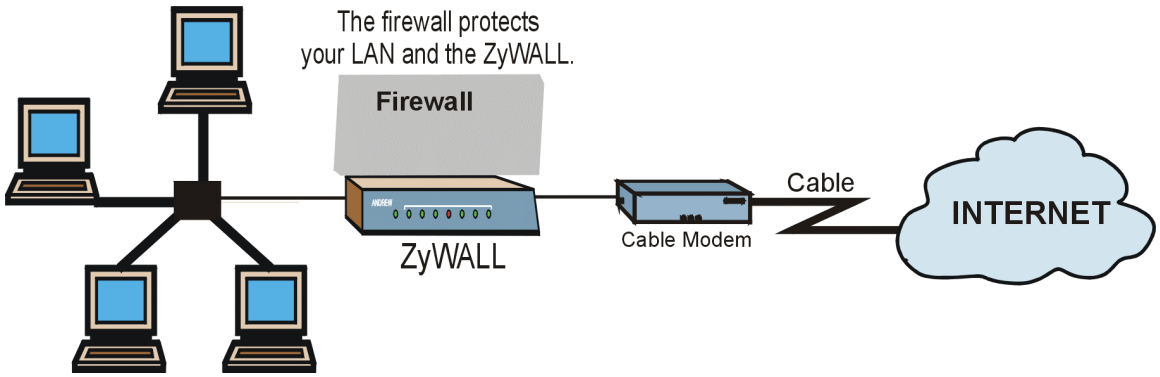


Figure 1-1 Secure Internet Access via Cable

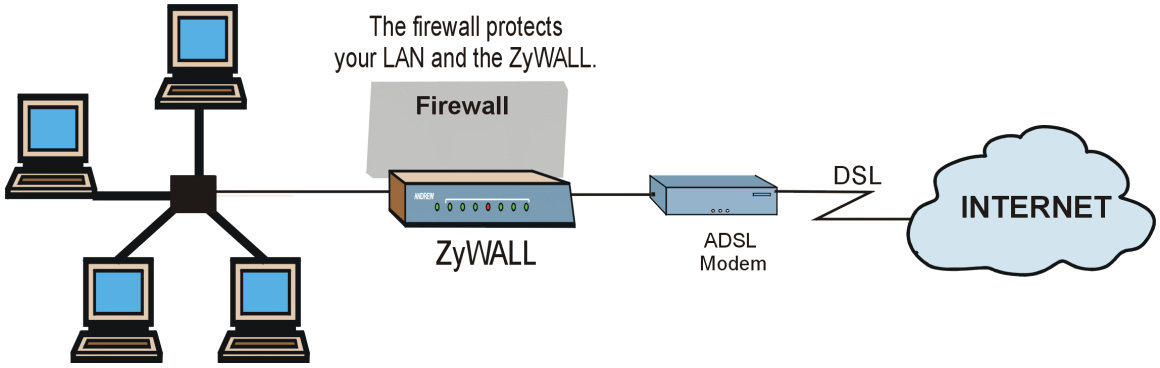


Figure 1-2 Secure Internet Access via DSL

You can also use your xDSL modem in the bridge mode for always-on Internet access and high-speed data transfer.

1.3.2 VPN Application

ZyWALL VPN is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) for leased lines between sites.

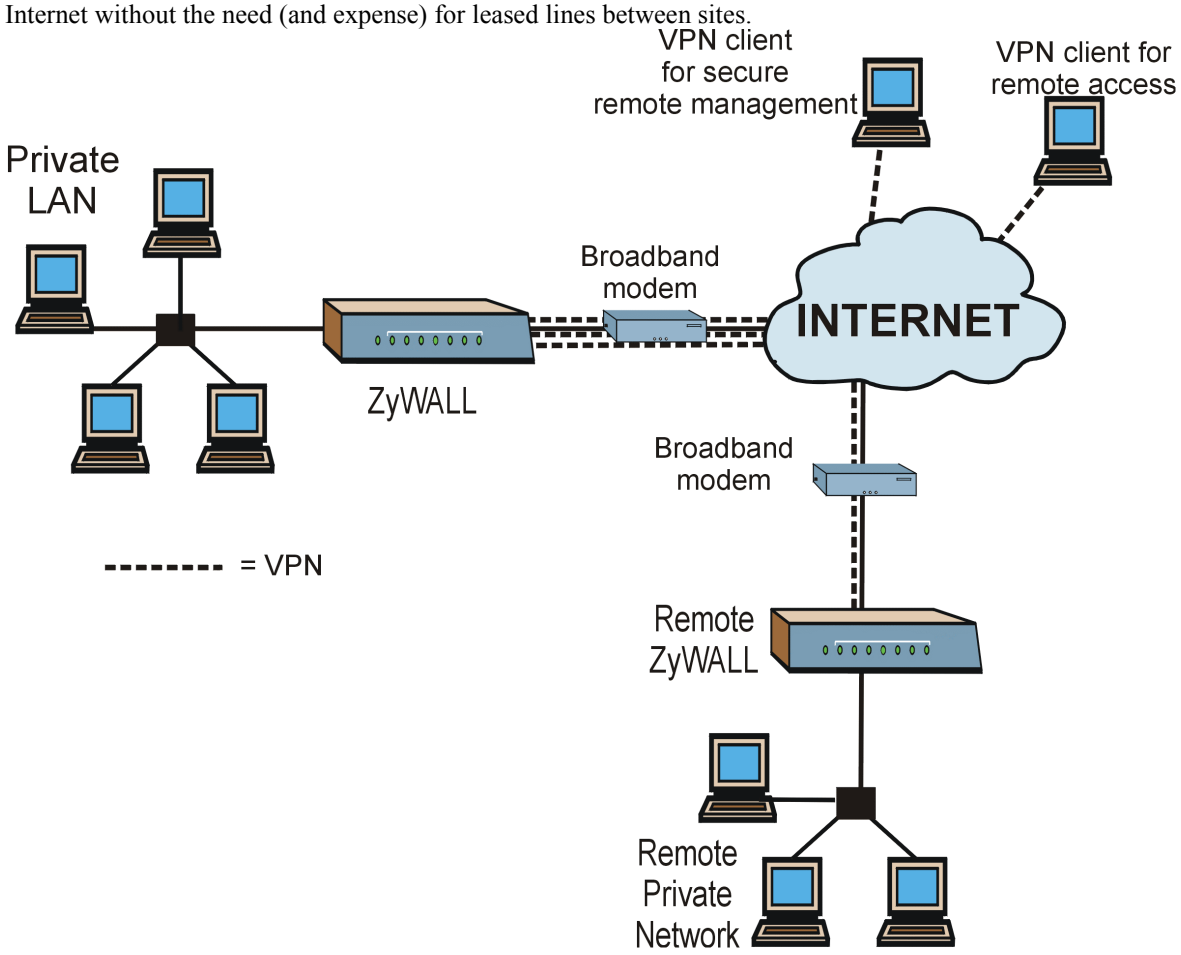


Figure 1-3 VPN Application

Chapter 2
Hardware Installation

This chapter explains the LEDs and ports as well as how to connect the hardware and perform the initial setup.

2.1 Front Panel LEDs and Back Panel Ports

2.1.1 Front Panel LEDs

The LEDs on the front panel indicate the operational status of the ZyWALL.

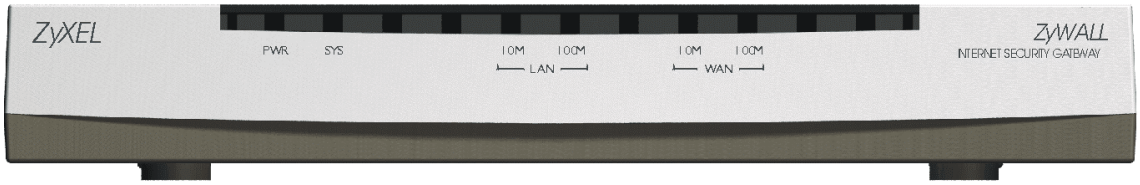


Figure 2-1 Front Panel

The following table describes LED functions.

Table 2-1 LED Descriptions

LED	FUNCTION	COLOR	STATUS	MEANING
PWR	Power	Green	On	The ZyWALL is turned on.
			Off	The ZyWALL is turned off.
SYS	System		Off	The system is not ready or failed.
			On	The system is ready and running.
			Flashing	The system is rebooting.
10M LAN	LAN	Green	Off	The 10M LAN is not connected.
			On	The ZyWALL is connected to a 10M LAN.

Table 2-1 LED Descriptions

LED	FUNCTION	COLOR	STATUS	MEANING
			Flashing	The 10M LAN is sending/receiving packets.
100M LAN	LAN	Orange	Off	The 100M LAN is not connected.
			On	The ZyWALL is connected to a 100Mbps LAN.
			Flashing	The 100M LAN is sending/receiving packets.
10M WAN	WAN	Green	Off	The 10M WAN is not connected.
			On	The ZyWALL is connected to a 10M WAN.
			Flashing	The 10M WAN is sending/receiving packets.
100M WAN	WAN	Orange	Off	The WAN Link is not ready, or has failed.
			On	The WAN Link is OK.
			Flashing	The 100M WAN link is sending/receiving packets.

2.2 ZyWALL 50 Rear Panel and Connections

The following figure shows the rear panel of your ZyWALL 50 and the related connections.

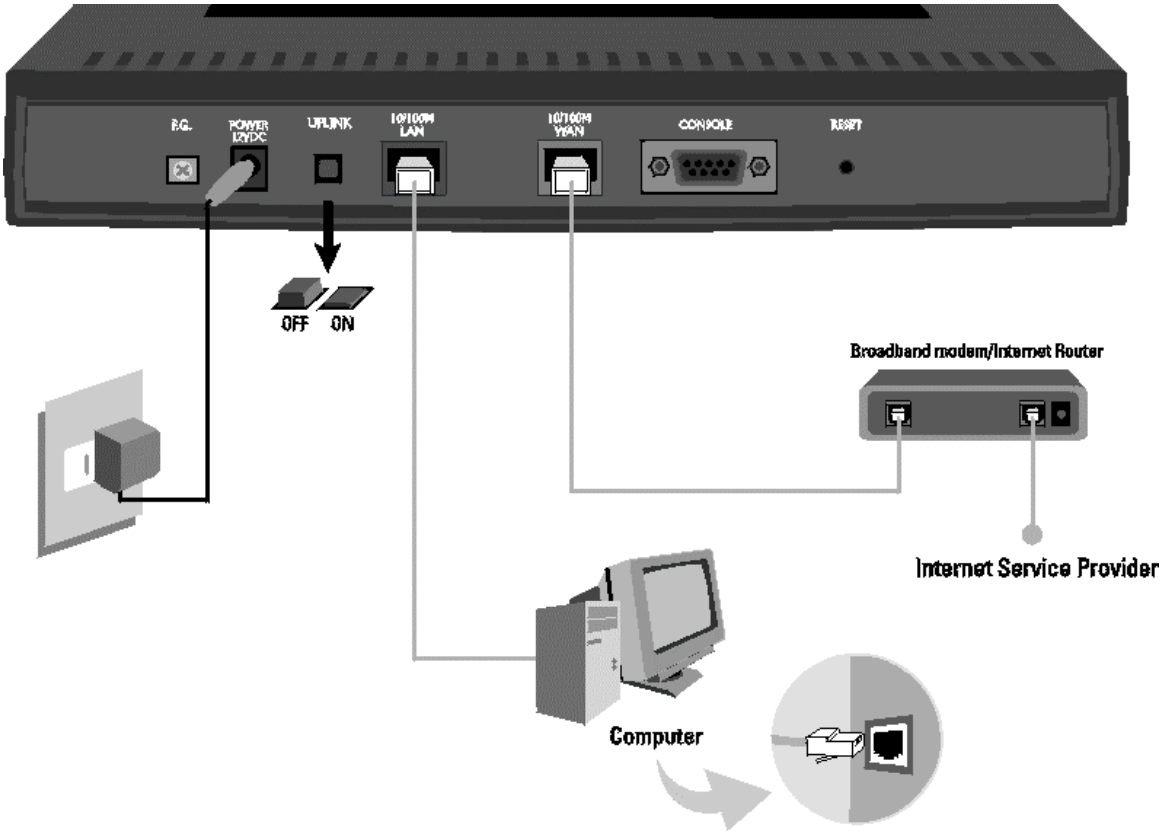


Figure 2-2 ZyWALL 50 Rear Panel and Connections

This section outlines how to connect your ZyWALL 50 to the LAN and the WAN. If you want to connect a cable modem you must connect the coaxial cable from your cable service to the threaded coaxial cable connector on the back of the cable modem. Connect an xDSL modem to the xDSL wall jack. See also the *Appendices* for important safety instructions when making connections to the ZyWALL.

Step 1. Connecting the Console Port

Use terminal emulator software on a computer when connecting a computer to the ZyWALL via the console port. Connect the 9-pin end of the console cable to the console port of the ZyWALL and the other end (choice of 9-pin or 25-pin, depending on your computer) to a serial port (COM1, COM2 or other COM

port) of your computer. You can use an extension RS-232 cable if the enclosed one is too short. After the initial setup, you can modify the configuration remotely through telnet connections.

Step 2. Connecting the ZyWALL to the Broadband Modem

Step 2a. Connecting the ZyWALL to the cable modem:

Connect the WAN port on the ZyWALL to the Ethernet port on the cable modem using the cable that came with your cable modem. The Ethernet port on a cable modem is sometimes labeled "PC" or "Workstation".

OR

Step 2b. Connecting the ZyWALL to the xDSL modem:

Connect the WAN port on the ZyWALL to the Ethernet port on the xDSL modem using the cable that came with your xDSL modem.

Step 3. Connecting the ZyWALL to the LAN

For a single computer, connect the 10/100M LAN port on the ZyWALL to the Network Adapter on the computer using the white straight-through cable and push in the Uplink button ("on"). If the Uplink button is not “on”, you must use a crossover cable for this connection.

If you have more than one computer, then you must use an external hub. Connect the 10/100M LAN port on the ZyWALL to a port on the hub using a straight-through Ethernet cable and make sure the Uplink button is "off".

Step 4. Connecting the Power Adapter to your ZyWALL

Connect one end of the power adapter to the port labeled **POWER** on the rear panel of your ZyWALL.

Caution: To prevent damage to the ZyWALL, first make sure you have the correct AC power adapter. See the *Power Adapter Specification Appendix* for regional specifications.

Step 5. Grounding the ZyWALL

To ground the ZyWALL, connect a grounded wire to the **F.G.** (Frame Ground) of the ZyWALL.

2.3 Additional Installation Requirements

In addition to the contents of your package, there are other hardware and software requirements you need before you can install and use your ZyWALL. These requirements include:

1. A computer with an Ethernet NIC (Network Interface Card) installed.
2. A computer equipped with communications software configured to the following parameters:
   - VT100 terminal emulation.
   - 9600 Baud.
   - No parity, 8 data bits, 1 stop bit, flow control set to none.
3. A cable/xDSL modem and an ISP account.

After the ZyWALL is properly set up, you can make future changes to the configuration through telnet or web connections.

To keep the ZyWALL operating at optimal internal temperature, keep the bottom, sides and rear clear of obstructions and away from the exhaust of other equipment.

Chapter 3
Initial Setup

This chapter explains how to perform initial ZyWALL setup and gives an overview of SMT menus.

3.1 Turning On Your ZyWALL

At this point, you should have connected the console port, the LAN port, the WAN port and the power port to the appropriate devices or lines. Plug the power adapter into a wall outlet. The PWR LED should turn on. The SYS LED will turn on after the system tests are complete. The WAN LED and one of the LAN LEDs should turn on immediately after the SYS LED turns on, if connections have been made to the LAN and WAN ports.

3.1.1 Initial Screen

When you turn on your ZyWALL, it performs several internal tests as well as line initialization.
After the tests, the ZyWALL asks you to press [ENTER] to continue, as shown next.

```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:41:51:61
initialize ch =1, ethernet address: 00:a0:c5:41:51:62
Press ENTER to continue...
```

Figure 3-1 Initial Screen

3.1.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below. For your first login, enter the default password “1234”. As you type the password, the screen displays an (X) for each character you type.
Please note that if there is no activity for longer than five minutes after you log in, your ZyWALL will automatically log you out and will display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

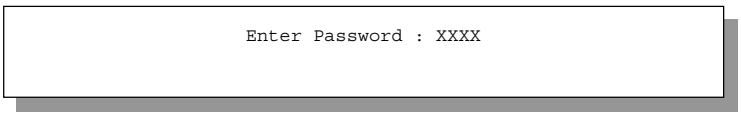


Figure 3-2 Password Screen

3.2 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyWALL. Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 3-1 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the “hidden” menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

3.2.1 Main Menu

After you enter the password, the SMT displays the **ZyWALL Main Menu**, as shown next.

```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.

                ZyWALL Main Menu

Getting Started            Advanced Management

  1. General Setup           21. Filter and Firewall Setup
  2. WAN Setup               22. SNMP Configuration
  3. LAN Setup               23. System Password
  4. Internet Access Setup   24. System Maintenance

Advanced Applications        26. Schedule Setup
  11. Remote Node Setup      27. VPN/IPSec Setup
  12. Static Routing Setup
  15. NAT Setup
                             99. Exit


                      Enter Menu Selection Number:
```

Figure 3-3 ZyWALL Main Menu

3.2.2 System Management Terminal Interface Summary

Table 3-2 Main Menu Summary

NO.	MENU TITLE	FUNCTION
1	General Setup	Use this menu to set up administrative information and dynamic DNS.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	LAN Setup	Use this menu to configure LAN DHCP and TCP/IP settings as well as apply LAN filters.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.

Table 3-2 Main Menu Summary

NO.	MENU TITLE	FUNCTION
23	System Password	Change your password in this menu (recommended).
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN/ IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this menu to exit (necessary for remote configuration).

3.2.3 SMT Menus at a Glance

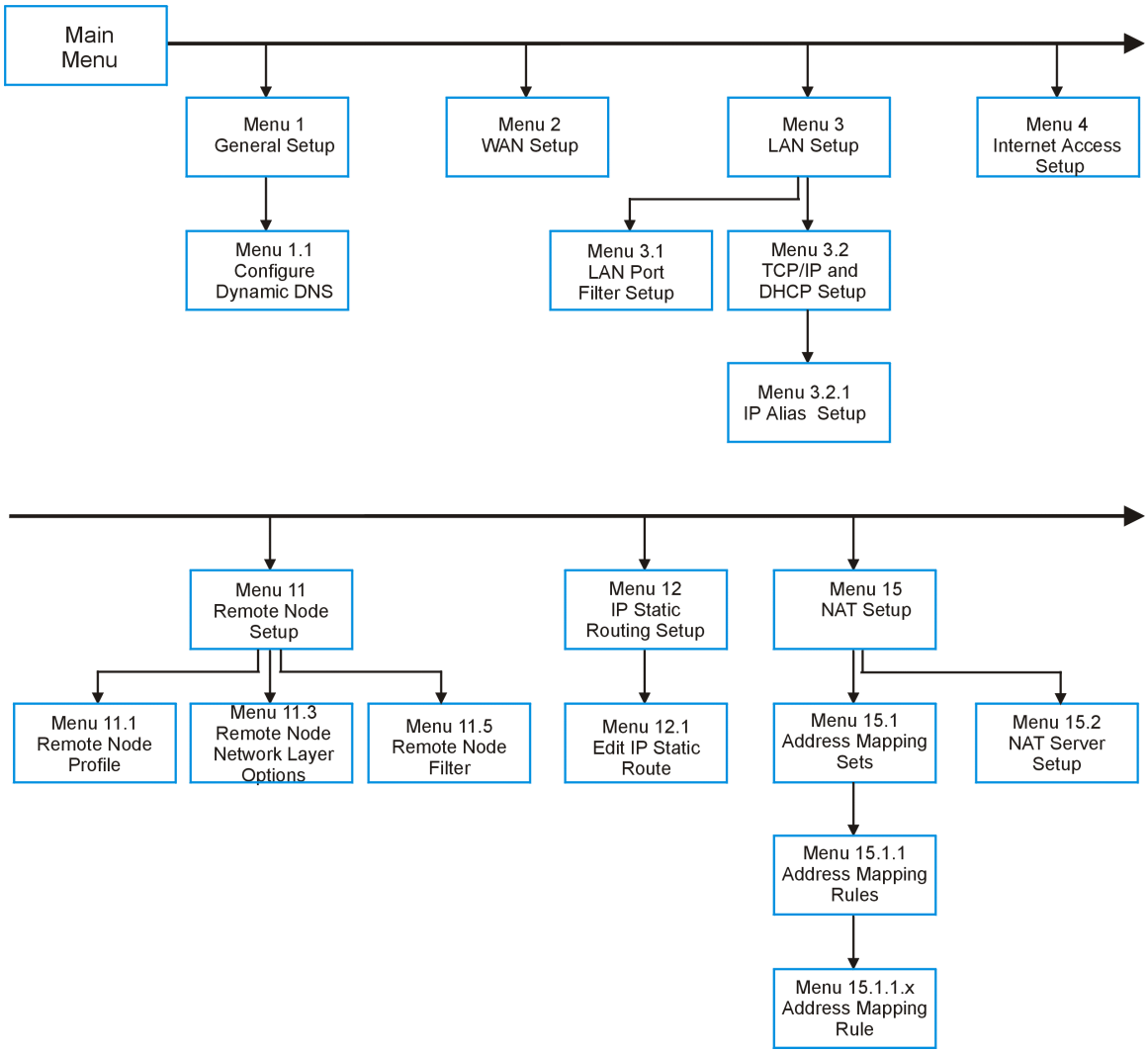

Main Menu
Menu 1 General Setup
Menu 2 WAN Setup
Menu 3 LAN Setup
Menu 4 Internet Access Setup
Menu 1.1 Configure Dynamic DNS
Menu 3.1 LAN Port Filter Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.2.1 IP Alias Setup
Menu 11 Remote Node Setup
Menu 12 IP Static Routing Setup
Menu 15 NAT Setup
Menu 11.1 Remote Node Profile
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 12.1 Edit IP Static Route
Menu 15.1 Address Mapping Sets
Menu 15.2 NAT Server Setup
Menu 15.1.1 Address Mapping Rules
Menu 15.1.1.x Address Mapping Rule

Figure 3-4 Getting Started and Advanced Applications SMT Menus

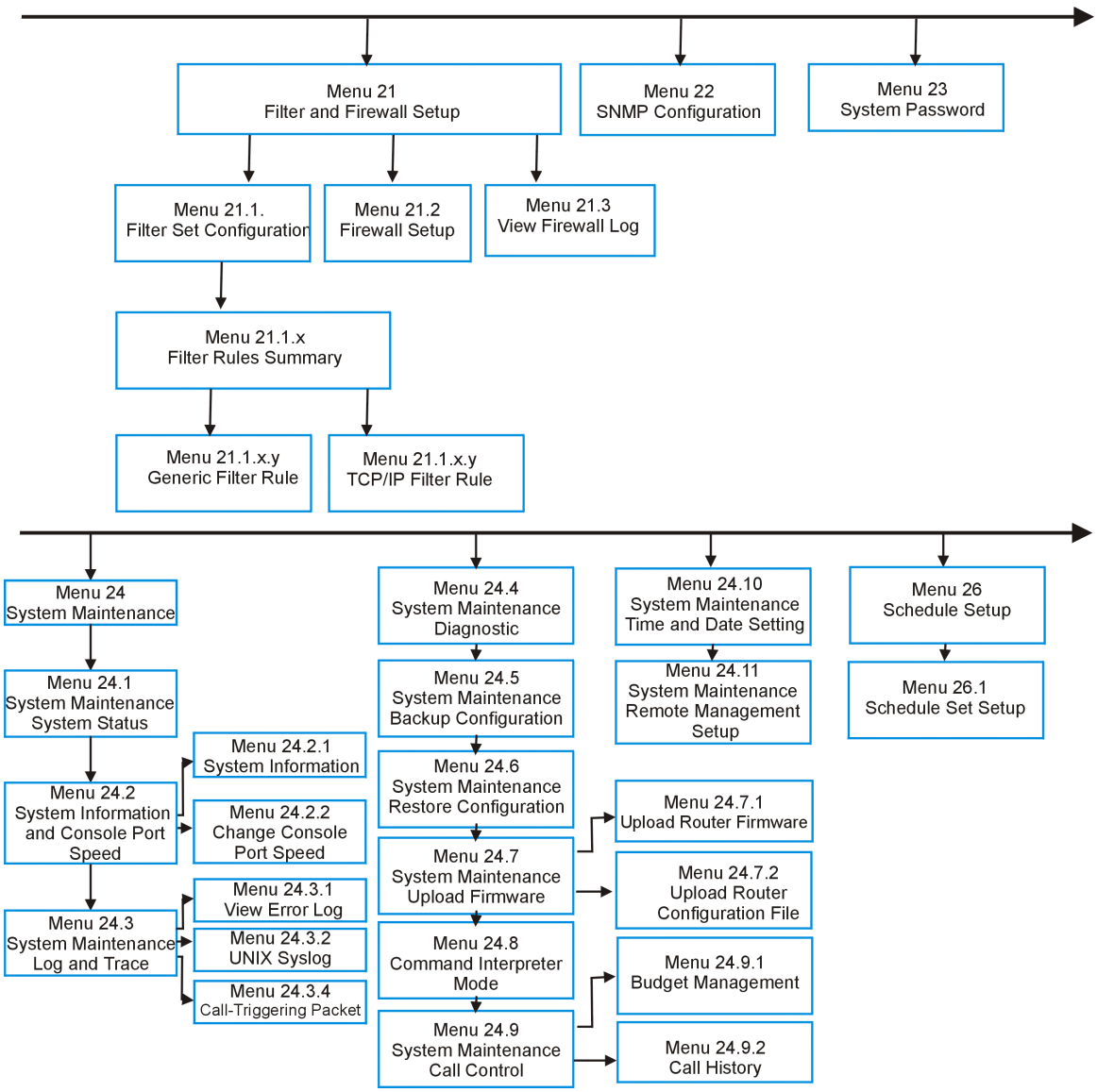


Figure 3-5 Advanced Management SMT Menus

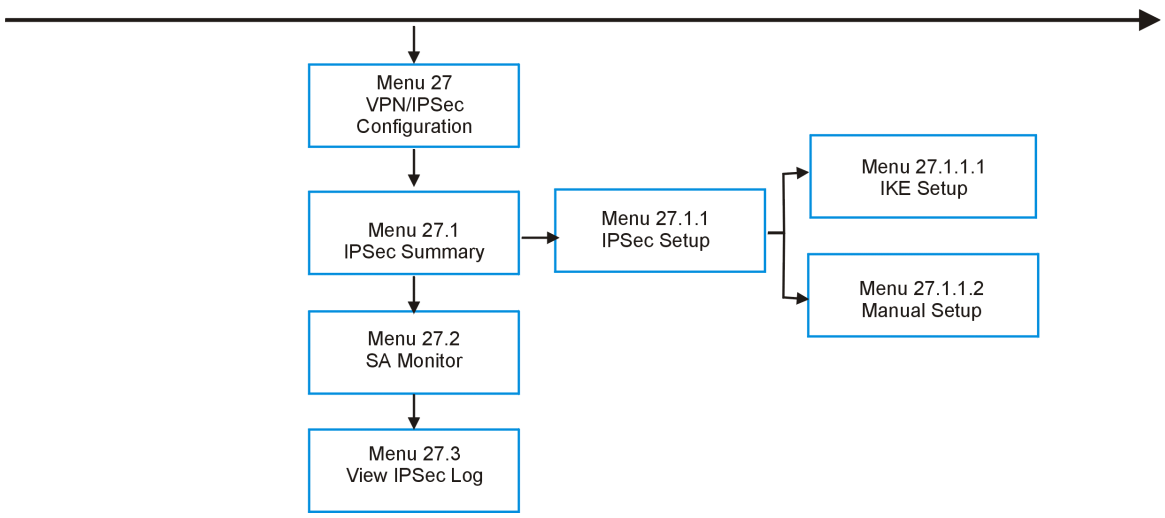


Figure 3-6 IPSec VPN Configuration SMT Menus

3.3 Changing the System Password

The first thing you should do is change the default system password by following the steps shown next.

Step 1. Enter 23 in the main menu to open **Menu 23 - System Password** as shown below.

```
                    Menu 23 - System Password


          Old Password= ?
          New Password= ?
          Retype to confirm= ?




            Enter here to CONFIRM or ESC to CANCEL:
```

Figure 3-7 Menu 23 — System Password

Step 2. Type in your existing password and press [ENTER].

Step 3. Type in your new system password and press [ENTER].

Step 4. Re-type your new system password for confirmation and press [ENTER].
Note that as you type a password, the screen displays an (X) for each character you type.

3.4 Resetting the ZyWALL

If you forget your password or cannot access the ZyWALL, you will need to reload the factory-default configuration file. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to "1234" and the LAN IP address to 192.168.1.1also.
To obtain the default configuration file, download it from the ZyXEL FTP site, unzip it and save it in a folder. Turn the ZyWALL off and then on to begin a session. When you turn on the ZyWALL again you will see the initial screen. When you see the message "Press any key to enter Debug Mode within 3 seconds" press any key to enter debug mode.
To upload the configuration file, do the following:

1. Type `atlc` after the `Enter Debug Mode` message.
2. Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.
3. After a successful firmware upload, type `atgo` to restart the ZyWALL.

The ZyWALL is now reinitialized with a default configuration file including the default password of "1234".

3.4.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in three ways:

1. Upload the default configuration file via the console port as described above. See later in this User's Guide for more information on how to transfer the configuration file to your ZyWALL using the SMT menus.
2. Use the **RESET** button on the rear panel of the ZyWALL (see the next section). Use this method for cases when the password or IP address of the ZyWALL is not known.
3. Use the web configurator to restore defaults (see the web configurator HTML help).

3.4.2 Procedure To Use The Reset Button

Make sure the **SYS** led is on (not blinking) before you begin this procedure.

1. Press the **RESET** button for ten seconds, then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.
2. Turn the ZyWALL off.
3. While pressing the **RESET** button, turn the ZyWALL on.
4. Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.
5. Release the **RESET** button and wait for the ZyWALL to finish restarting.

Chapter 4
General And WAN Setup

__Menu 1 - General Setup__ contains administrative and system-related information. Clone a LAN computer MAC address in the __Menu 2 - WAN Setup__.

4.1 System Name

System Name is for identification purposes. ZyXEL recommends you enter your computer's "Computer name".

- In Windows 95/98 click **Start** -> **Settings** -> **Control Panel** and then double-click **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the ZyWALL **System Name**.
- In Windows 2000 click **Start**->**Settings**->**Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the ZyWALL **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this field blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (**System Name**) on each individual computer, the domain name can be assigned from the ZyWALL via DHCP.

4.2 Dynamic DNS

Dynamic DNS (Domain Name System) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in *NetMeeting*, *CU-SeeMe* or other services). You can also access your FTP server or Web site on your own computer using a DNS-like address (for example, *myhost.dhs.org*, where *myhost* is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name.
To use this service, you must register with the Dynamic DNS service provider. The Dynamic DNS service provider will give you a password or key. The ZyWALL supports www.dyndns.org. You can apply to this service provider for Dynamic DNS service.

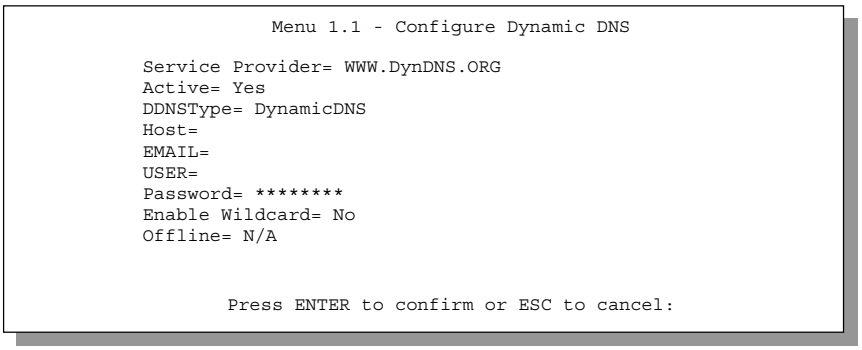


Figure 4-1 Configure Dynamic DNS

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 4-1 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s). Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org. At the time of writing, dyndns.org provides the basic **DynamicDNS** and **StaticDNS** services along with a limited number of hostnames for free, but charges a fee for **CustomDNS**. See www.dyndns.org for details.	**DynamicDNS** (defautl)

FIELD	DESCRIPTION	EXAMPLE
Host	Enter the domain name assigned to your ZyWALL by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your ZyWALL supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	**No**
Offline	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).	**Yes**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

The IP address will be updated when you reconfigure menu 1 or perform DHCP client renewal.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

4.3 WAN Setup

This section describes how to configure the WAN using **Menu 2 — WAN Setup**. From the main menu, enter 2 to open menu 2.

ZyXEL recommends you configure this menu even if your ISP does not require MAC address authentication.

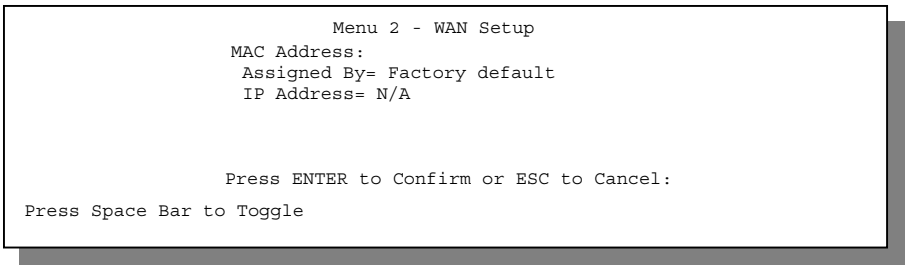

Menu 2 - WAN Setup
MAC Address:
Assigned By= Factory default
IP Address= N/A
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle

Figure 4-2 Menu 2 — WAN Setup

The MAC address field allows users to configure the WAN port's MAC address by using either the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting in menu 2 or upload a different rom file.

The following table contains instructions on how to configure your WAN setup.

Table 4-2 WAN Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
MAC Address		
Assigned By	Press [SPACE BAR] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP Address attached on LAN** to use the MAC Address of that computer whose IP you give in the following field.	**Factory default**
IP Address	This field is applicable only if you choose the **IP Address attached on LAN** method. Enter the IP address of the computer on the LAN whose MAC you are cloning.	N/A
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 5
LAN Setup

*This chapter describes how to configure the LAN using **Menu 3 – LAN Setup**.*

5.1 Introduction

This section describes how to configure the LAN using **Menu 3 — LAN Setup**. From the main menu, enter 3 to open menu 3.

```
                    Menu 3 - LAN Setup

                    1.  LAN Port Filter Setup
                    2.  TCP/IP and DHCP Setup


                Enter Menu Selection Number:
```

Figure 5-1 Menu 3 — LAN Setup

5.2 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Menu 3.2 is discussed in the next chapter. Please read on.

```
                Menu 3.1 - LAN Port Filter Setup

            Input Filter Sets:
               protocol filters= 2
               device filters=
            Output Filter Sets:
               protocol filters=
               device filters=


            Press ENTER to Confirm or ESC to Cancel:
```

Figure 5-2 Menu 3.1 — LAN Port Filter Setup

5.3 TCP/IP and DHCP for LAN

The ZyWALL has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

5.3.1 Factory LAN Defaults

The LAN parameters of the ZyWALL are preset in the factory with the following values:

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you an explicit DNS server address(es), skip ahead to section *5.4* to see how to enter the DNS server address(es).

5.3.2 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the workstation must be manually configured.

IP Pool Setup

The ZyWALL is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the ZyWALL itself) in the lower range for other server machines, e.g., server for mail, FTP, Telnet, web, etc., that you may have.

DNS Server Address

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.
There are two ways that an ISP disseminates the DNS server addresses.
The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in DHCP Setup**.**
The second is to leave this field blank, i.e., 0.0.0.0 — in this case, the ZyWALL acts as a DNS proxy.

Table 5-1 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2 - 192.168.1.32**;** 192.168.1.65 - 192.168.1.254
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1 (ZyWALL LAN IP address)

5.3.3 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.
If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyWALL. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual workstation on that network.
Once you have decided on the network number, pick an IP address that is easy to remember, e.g., 192.168.1.1, for your ZyWALL, but make sure that no other device on your network is using that IP.
The subnet mask specifies the network number portion of an IP address. Your ZyWALL will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyWALL unless you are instructed to do otherwise.

5.3.4 Private IP Addresses

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, e.g., only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

Table 5-2 Private IP Address Ranges

10.0.0.0 — 10.255.255.255
172.16.0.0 — 172.31.255.255
192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

5.3.5 RIP Setup

RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.
Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
By default, **RIP Direction** is set to **Both** and the **Version** set to **RIP-1**.

5.3.6 IP Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender — 1 recipient) or Broadcast (1 sender — everybody on the network). Multicast delivers IP packets to *a group* of hosts on the network - not everybody and not just 1.
IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.
The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyWALL queries all directly connected networks to gather group membership. After that, the ZyWALL periodically updates this information. IP Multicasting can be enabled/disabled on the ZyWALL LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

5.3.7 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network.

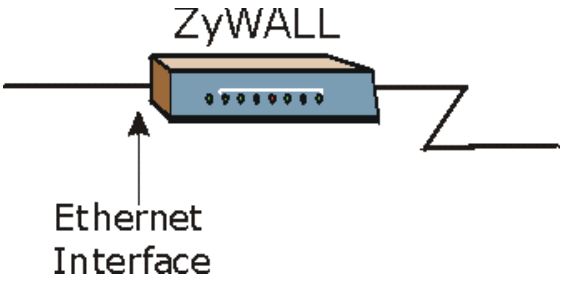


Figure 5-3 Physical Network

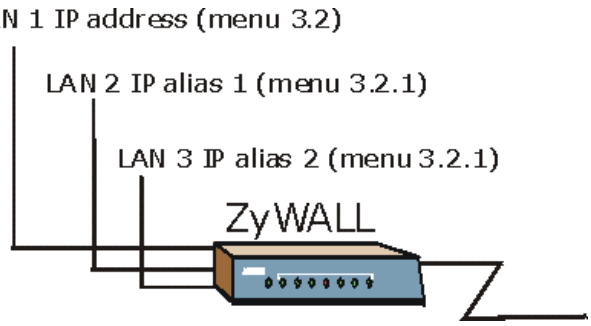


Figure 5-4 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your ZyWALL.

5.4 TCP/IP and DHCP Ethernet Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.

```
                    Menu 3 - LAN Setup


        1.  LAN Port Filter Setup
        2.  TCP/IP and DHCP Setup



Enter Menu Selection Number:
```

Figure 5-5 Menu 3 — TCP/IP and DHCP Setup

From menu 3, select the submenu option **TCP/IP and DHCP** and press [ENTER]. The screen now displays **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next.

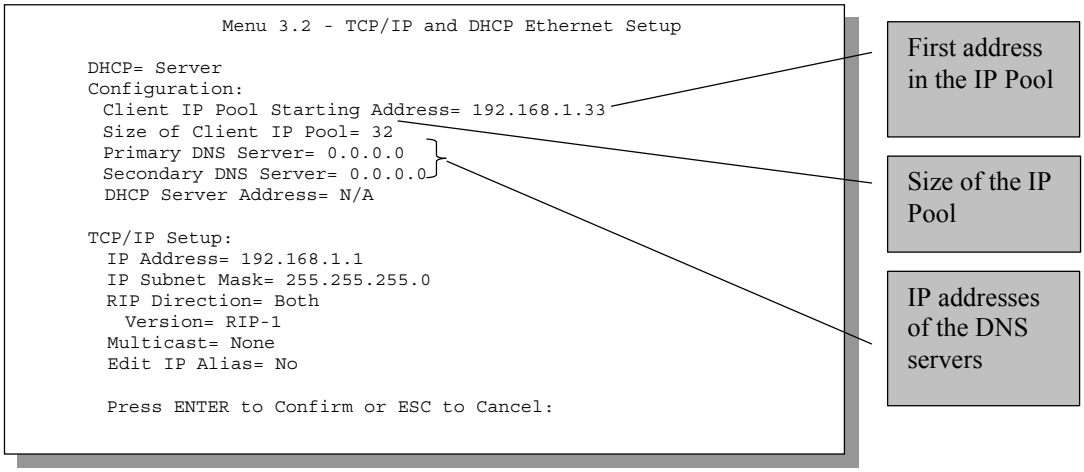

Menu 3.2 - TCP/IP and DHCP Ethernet Setup
DHCP= Server
Configuration:
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
DHCP Server Address= N/A
TCP/IP Setup:
IP Address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-1
Multicast= None
Edit IP Alias= No
Press ENTER to Confirm or ESC to Cancel:
First address in the IP Pool
Size of the IP Pool
IP addresses of the DNS servers

Figure 5-6 Menu 3.2 — TCP/IP and DHCP Ethernet Setup

Follow the instructions in the next table on how to configure the DHCP fields.

Table 5-3 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP	This field enables/disables the DHCP server. If set to **Server**, your ZyWALL will act as a DHCP server. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyWALL acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to **Server**, the following four items need to be set:	**Server**
Configuration:		
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	32
Primary DNS Server	Type in the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Secondary DNS Server		

Table 5-3 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Server Address	If **Relay** is selected in the **DHCP** field above, then type in the IP address of the actual, remote DHCP server here.	

Follow the instructions in the following table to configure TCP/IP parameters for the LAN port.

Table 5-4 LAN TCP/IP Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup:		
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] to enable IP Multicasting or select **None** (default) to disable it.	**None**
Edit IP Alias	The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes**, then press [ENTER] to display menu 3.2.1	**Yes**
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

5.4.1 IP Alias Setup

Use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.
Pressing [ENTER] opens **Menu 3.2.1 - IP Alias Setup**, as shown next.

```
                          Menu 3.2.1 - IP Alias Setup

                        IP Alias 1= No
                          IP Address= N/A
                          IP Subnet Mask= N/A
                          RIP Direction= N/A
                            Version= N/A
                          Incoming protocol filters= N/A
                          Outgoing protocol filters= N/A
                        IP Alias 2= No
                          IP Address= N/A
                          IP Subnet Mask= N/A
                          RIP Direction= N/A
                            Version= N/A
                          Incoming protocol filters= N/A
                          Outgoing protocol filters= N/A

                         Enter here to CONFIRM or ESC to CANCEL:

    Press Space Bar to Toggle.
```

Figure 5-7 Menu 3.2.1 — IP Alias Setup

Use the instructions in the following table to configure IP Alias parameters.

Table 5-5 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose **Yes** to configure the LAN network for the ZyWALL.	**Yes**
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.	192.168.2.1
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.	**None**
Version	Press [SPACE BAR] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL.	2
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

Chapter 6
Internet Access

This chapter shows you how to configure your ZyWALL for Internet access.

6.1 Internet Access Setup

You will see three different menu 4 screens depending on whether you chose **Ethernet, PPTP** or **PPPoE Encapsulation**.

6.1.1 Ethernet Encapsulation

You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The PPPoE choice is for a dial-up connection using PPPoE. If you choose **Ethernet** in menu 4 you will see the next screen.

```
            Menu 4 - Internet Access Setup

        ISP's Name= ChangeMe
        Encapsulation= Ethernet
          Service Type= Standard
          My Login= N/A
          My Password= N/A
          Login Server IP= N/A

        IP Address Assignment= Dynamic
          IP Address= N/A
          IP Subnet Mask= N/A
          Gateway IP Address= N/A
        Network Address Translation= SUA Only




         Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-1 Menu 4 — Internet Access Setup (Ethernet)

The following table describes this screen.

Table 6-1 Internet Access Setup Menu Fields

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.

Table 6-1 Internet Access Setup Menu Fields

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for IP Address.
Service Type	Press [SPACE BAR] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Note: xDSL users must choose the **Standard** option only. The **Server IP**, **My Login IP** and **My Password** fields are not applicable in this case.	
My Login Name	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Login Server IP	The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
IP Address Assignment	If your ISP did not assign you a fixed IP address, select **Dynamic**, otherwise select **Static** and enter the IP address & subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (Static IP Address Assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature. The choices are **Full Feature**, **None** and **SUA Only**.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

6.1.2 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

The ZyWALL 50 supports one PPTP server connection at any given time.

6.1.3 Configuring the PPTP Client

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

```
                Menu 4 - Internet Access Setup

            ISP's Name= ChangeMe
            Encapsulation= PPTP
              Service Type= N/A
              My Login=
              My Password= ******
              Idle Timeout= 100

             IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Address=N/A
             Network Address Translation= SUA Only


           Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-2 Internet Access Setup (PPTP)

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 6-2 New Fields in Menu 4 (PPTP) screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for IP Address.	**PPTP**
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server.	100 (default)

6.1.4 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (e.g., Radius). For the user, PPPoE provides a login & authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.
Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyWALL 50 (rather than individual computer's), the computers on the LAN do not need PPPoE software installed, since the ZyWALL does that part of the task. Furthermore, with NAT, all of the LAN's computers will have access.

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see *the Appendices*.

```
                Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPPoE
  Service Type=
  My Login=
  My Password= ********
  Idle Timeout= 100

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only


Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-3 Internet Access Setup (PPPoE)

Table 6-3 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The	**PPPoE**

Table 6-3 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices for IP Address.	**PPPoE**
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server.	100 (default)

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

6.2 Basic Setup Complete

Well done! You have successfully connected, installed and set up your ZyWALL to operate on your network as well as access the Internet.

When the firewall is activated the default policy allows all communications to the Internet that originate from the LAN and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the ZyWALL web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the *firewall part*.

Part II:

Advanced Applications

This part covers Remote Node Setup, IP Static Route Setup and Network Address Translation.

Chapter 4
Remote Node Setup

This chapter shows you how to configure a remote node.

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. We will show you how to configure **Menu 11.1 Remote Node Profile, Menu 11.3 - Remote Node Network Layer Options** and **Menu 11.5 - Remote Node Filter**.

4.1 Remote Node Profile

From the main menu, select menu option 11 to open **Menu 11.1 - Remote Node Profile**. There are two variations of this menu depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation.**

4.1.1 Ethernet Encapsulation

You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

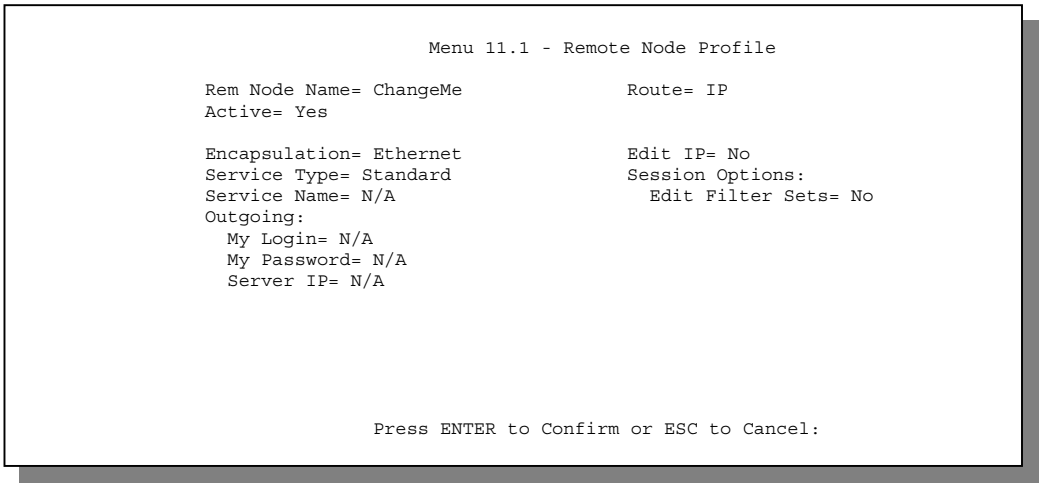


Figure 4-1 Menu 11.1 — Remote Node Profile for Ethernet Encapsulation

Table 4-1 Fields in Menu 11.1

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] to select **Yes** (activate remote node) or **No** (deactivate remote node).	**Yes**
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] if you wish to change to **PPPoE** encapsulation.	**Ethernet**
Service Type	Press [SPACE BAR] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.	**Standard**
Service Name	This is valid only when you have chosen **PPPoE** encapsulation. If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here.	poellc
Outgoing My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.	**jim**

Table 4-1 Fields in Menu 11.1

FIELD	DESCRIPTION	EXAMPLE
My Password Server IP	Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for **PPPoE** encapsulation only. This field is valid for RoadRunner service type only. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	*****
Route	This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL 50.	**IP**
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**.	**Yes**
Session Options Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**Yes**
Once you have configured the Remote Node Profile Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

4.1.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the ZyWALL with an xDSL modem as the WAN device. If you change the Encapsulation to **PPPoE,** then you will see the next screen. Please see the *Appendices* for more information on PPPoE.

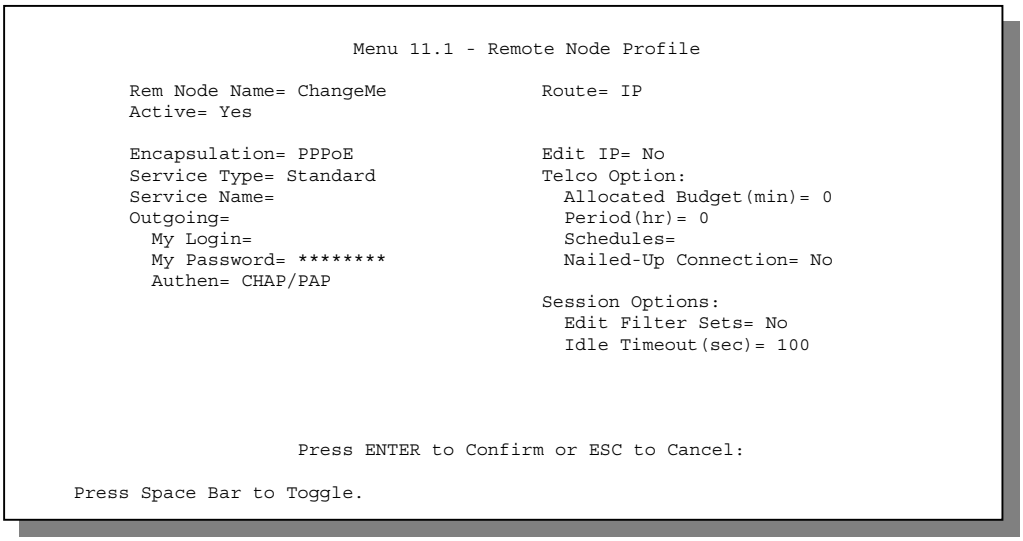


Figure 4-2 Menu 11.1 — Remote Node Profile for PPPoE Encapsulation

Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter the case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyWALL does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyWALL will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in *Table 4-1*.

Table 4-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION	EXAMPLE
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP**
Telco Option		
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	10
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour).	1
Schedules	You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup chapter*.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options Idle Timeout	This value specifies the idle time (i.e., the length of time there is no traffic from the ZyWALL to the remote node) in seconds that can elapse before the ZyWALL automatically disconnects the PPPoE connection. *This option only applies when the ZyWALL initiates the call.*	100 seconds (default)

4.1.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the A*ppendices* for information on PPTP.

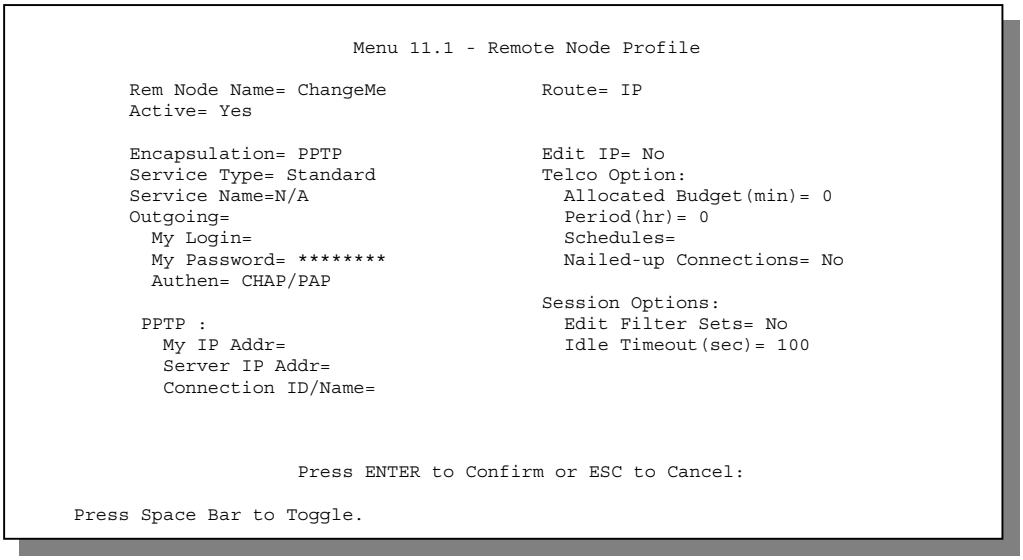


Figure 4-3 Menu 11.1 — Remote Node Profile for PPTP Encapsulation

The next table shows how to configure fields in menu 11.1 not previously discussed above.

Table 4-3 Fields in Menu 11.1 (PPTP Encapsulation)

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Toggle the space bar to choose **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	**PPTP**
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format. This field is optional and depends on the requirements of your xDSL Modem.	n:My ISP
Schedules	You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Setup* chapter.	
Nailed-Up Connections	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node a nailed-up connection.	**No**

4.2 Editing TCP/IP Options (with Ethernet Encapsulation)

Move the cursor to the **Edit IP** field in menu 11.1, press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.

```
                Menu 11.3 - Remote Node Network Layer Options

                       IP Address Assignment= Dynamic
                       IP Address= N/A
                       IP Subnet Mask= N/A
                       Gateway IP Addr= N/A

      Network Address Translation= SUA Only
                       Metric= N/A
                       Private= N/A
                       RIP Direction= None
                         Version= N/A
                       Multicast= None

                        Enter here to CONFIRM or ESC to CANCEL:
   Press Space Bar to Toggle
```

Figure 4-4 Menu 11.3 — Remote Node Network Layer Options

The next table gives you instructions about configuring remote node network layer options.

Table 4-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic**
IP Address	If you have a Static IP Assignment, enter the IP address assigned to you by your ISP.	
IP Subnet Mask	If you have a Static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	If you have a Static IP Assignment, enter the gateway IP address assigned to you.	
Network Address Translation	Use [SPACE BAR] to select either **Full Feature**, **None** or **SUA Only**. See the *NAT chapter* for a full discussion on this feature.	**SUA Only**
Metric	This field is valid only for PPTP/PPPoE encapsulation. The metric represents the “cost” of transmission for routing purposes. IP routing	3

Table 4-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Metric	This field is valid only for PPTP/PPPoE encapsulation. The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	3
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**Yes**
RIP	Press [SPACE BAR] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. Please see the *RIP Setup section* for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.	**None**
Version	Press [SPACE BAR] to select the RIP version from **RIP-1**/**RIP-2B**/**RIP-2M** or **None**.	N/A
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2)**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the previous *Part* for more information on this feature.	**None**
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

4.2.1 Editing TCP/IP Options (with PPTP Encapsulation)

Make sure that **Encapsulation** is set to **PPTP** in menu 11.1. Then move the cursor to the **Edit IP** field in menu 11.1, press the [SPACE BAR] to toggle **No** to **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.

```
            Menu 11.3 - Remote Node Network Layer Options

                        IP Address Assignment= Dynamic
                        Rem IP Address= N/A
                        Rem Subnet Mask= N/A
                        My WAN Addr= 0.0.0.0

                        Network Address Translation= Full Feature
                        Metric= 1
                        Private= No
                        RIP Direction= None
                          Version= N/A
                        Multicast= None

                         Enter here to CONFIRM or ESC to CANCEL:
    Press Space Bar to Toggle.
```

Figure 4-5 Menu 11.3 — Remote Node Network Layer Options

The next table gives you instructions about configuring remote node network layer options.

Table 4-5 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic**
Rem IP Address	If you have a **Static IP Assignment**, enter the IP address assigned to the remote node.	192.168.1.1
Rem IP Subnet Mask	If you have a **Static IP Assignment**, enter the subnet mask assigned to the remote node.	255.255.255.0
My WAN Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyWALL. Note that this is the address assigned to your local ZyWALL, not the remote router.	0.0.0.0
Network Address Translation	Use [SPACE BAR] to select either **Full Feature, None** or **SUA Only.** See the *NAT chapter* for a full discussion on this feature.	**SUA Only**
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise,	1 to 15

Table 4-5 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	1 to 15
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**Yes**
RIP Version	Press [SPACE BAR] to select the **RIP direction** from **Both/ None/In Only/Out Only** and **None**. Press [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**None** (default) **RIP-1**
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the previous Part for more information on this feature.	**None**
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

4.2.2 Editing TCP/IP Options (with PPPoE Encapsulation)

Make sure **Encapsulation** is set to **PPPoE** in menu 11.1. Move the cursor to the **Edit IP** field in **Menu 11.1** and press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**. The menu and fields are the same as described for PPTP encapsulation above.

4.3 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, e.g., 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to the *Filters chapter*. For PPPoE or PPTP encapsulation, you can also specify remote node call filter sets.

```
                    Menu 11.5 - Remote Node Filter

                Input Filter Sets:
                  protocol filters= 3
                    device filters=
                Output Filter Sets:
                  protocol filters= 1
                    device filters=

                 Enter here to CONFIRM or ESC to CANCEL:
```

Figure 4-6 Menu 11.5 — Remote Node Filter (Ethernet Encapsulation)

```
                Menu 11.5 - Remote Node Filter

                Input Filter Sets:
                  protocol filters= 3
                    Device filters=
                Output Filter Sets:
                  protocol filters= 1
                    device filters=
                Call Filter Sets:
                  protocol filters= 1
                    Device filters=




                 Enter here to CONFIRM or ESC to CANCEL:
```

Figure 4-7 Menu 11.5 — Remote Node Filter (PPPoE or PPTP Encapsulation)

Chapter 5
IP Static Route Setup

This chapter shows you how to configure static routes with your ZyWALL.

Static routes tell the ZyWALL routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN.

Each remote node specifies only the network to which the gateway is directly connected, and the ZyWALL has no knowledge of the networks beyond. For instance, the ZyWALL knows about network N2 in the following diagram through remote node Router 1. However, the ZyWALL is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyWALL about the networks beyond the remote nodes.

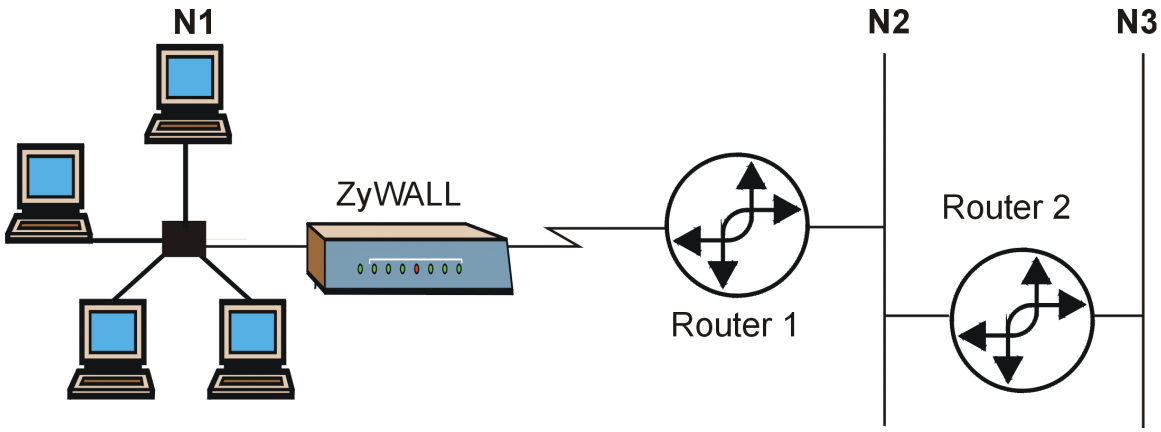


Figure 5-1 Example of Static Routing Topology

5.1 IP Static Route Setup

You configure IP static routes in menu 12. 1 by selecting one of the IP static routes as shown next. Enter 12 from the main menu.

```
                    Menu 12 - IP Static Route Setup

                1. ________
                2. ________
                3. ________
                4. ________
                5. ________
                6. ________
                7. ________
                8. ________




                              Enter selection number:
```

Figure 5-2 Menu 12 — IP Static Route Setup

Now, enter the index number of one of the static routes you want to configure.

```
                  Menu 12.1 - Edit IP Static Route


                    Route #: 1
                    Route Name= ?
                    Active= No
                    Destination IP Address= ?
                    IP Subnet Mask= ?
                    Gateway IP Address= ?
                    Metric= 2
                    Private= No

Press ENTER to CONFIRM or ESC to CANCEL:
```

Figure 5-3 Menu 12. 1 — Edit IP Static Route

`The following table describes the IP Static Route Menu fields.

Table 5-1 IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

Chapter 6
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

6.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, e.g., the source address of an outgoing packet, used within one network to a different IP address known within another network.

6.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyWALL, e.g., the workstations of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, e.g., the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is travelling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 6-1 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Table 6-1 NAT Definitions

TERM	DESCRIPTION
	WAN.

NAT never changes the IP address (either local or global) of an outside **host.**

6.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 6-2*), NAT offers the additional benefit of firewall protection. If no server is defined in these cases, all incoming inquiries will be filtered out by your ZyWALL, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT).*

6.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

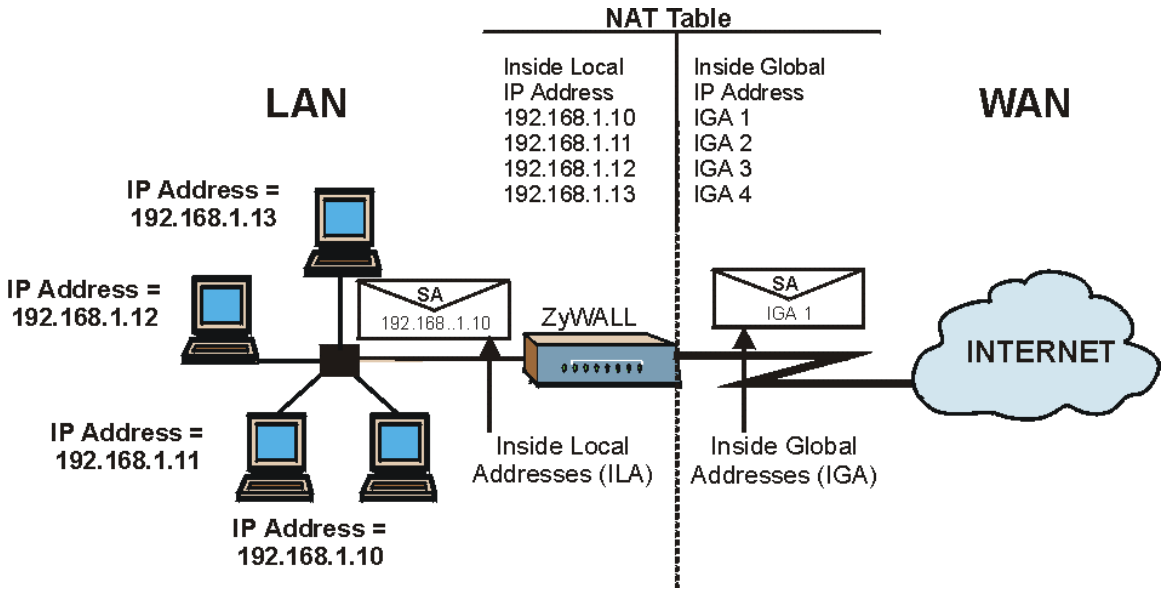


Figure 6-1 How NAT Works

6.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyWALL can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

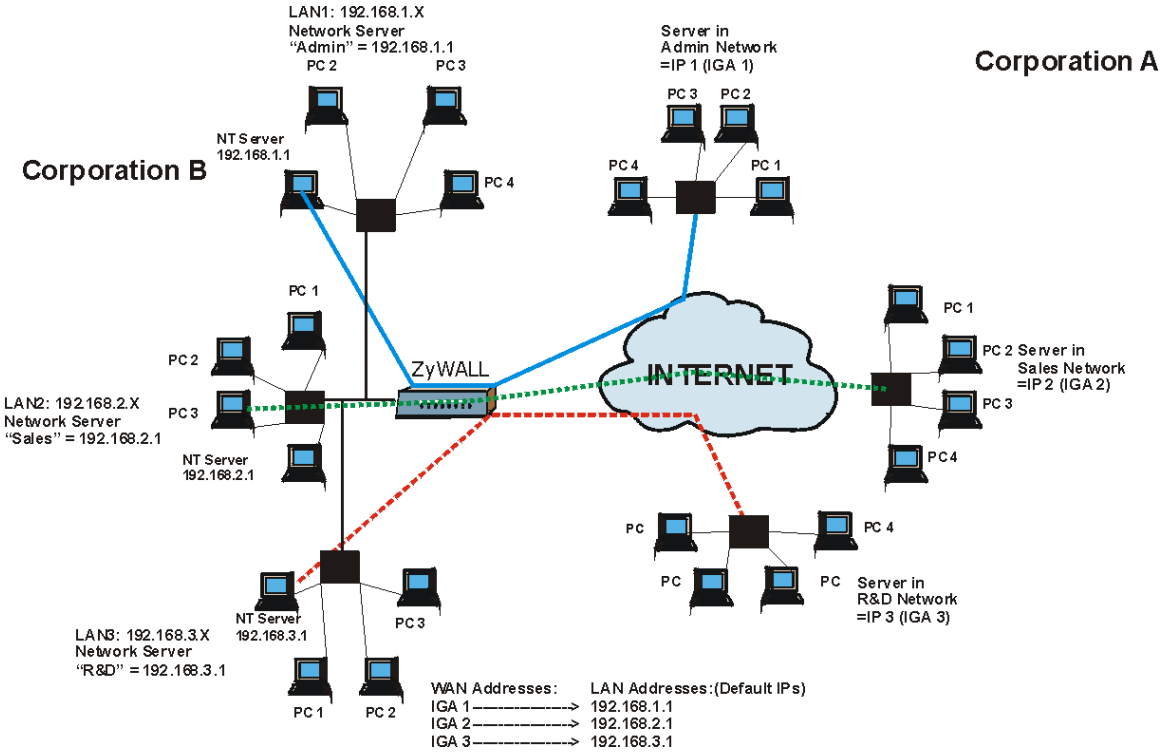


Figure 6-2 NAT Application With IP Alias

6.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

1. **One to One**: In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
2. **Many to One**: In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the SUA Only option in today's routers).

3. **Many to Many Overload**: In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
4. **Many to Many No Overload**: In Many-to-Many No Overload mode, the ZyWALL maps the each local IP addresses to unique global IP addresses.
5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do not **change for** One-to-One **and** Many-to-Many-No Overload **NAT mapping types.**

The following table summarizes these types.

Table 6-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M:M No Ov
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

6.2 Using NAT

6.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section *6.3.1* for a detailed description of the NAT set for SUA. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 6-2*.

1. **Choose** SUA Only **if you have just one public WAN IP address for your ZyWALL.**
2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your ZyWALL.**

6.2.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

```
                Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Login Server IP= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only



Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-3 Menu 4 — Applying NAT for Internet Access

The following figure shows how you apply NAT to the remote node in menu 11.1.

Step 1. Enter 11 from the main menu.

Step 2. Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

```
            Menu 11.3 - Remote Node Network Layer Options

              IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Addr= N/A

              Network Address Translation= SUA Only
              Metric= N/A
              Private= N/A
              RIP Direction= None
                Version= N/A
              Multicast= None




          Enter here to CONFIRM or ESC to CANCEL:

          Press Space Bar to Toggle.
```

Figure 6-4 Menu 11.3 — Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

Table 6-3 Applying NAT in Menus 4 & 11.3

FIELD	OPTIONS	DESCRIPTION
Network Address Translation	**Full Feature**	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see section 6.3.1 for further discussion). You can configure any of the mapping types described in Table 6-2. Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL.
	None	NAT is disabled when you select this option.
	SUA Only	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see section *6.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL.

6.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in Table 6-2. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

A server set is a list of LAN side servers mapped to external ports. To use this set (one set for the ZyWALL 50), a server rule must be set up inside the NAT Address Mapping set. Please see *section 6.4* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

```
                    Menu 15 — NAT Setup

          1.    Address Mapping Sets
          2.    Server Set


                Enter Menu Selection Number:
```

Figure 6-5 Menu 15 — NAT Setup

6.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

```
                  Menu 15.1 — Address Mapping Sets

            1. NAT_SET
          255. SUA (read only)









              Enter Menu Selection Number:
```

Figure 6-6 Menu 15.1 — Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 6.2.1)*. The fields in this menu cannot be changed.

```
                        Menu 15.1.255 - Address Mapping Rules

 Set Name= SUA

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                    0.0.0.0                           Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.


                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-7 Menu 15.1.255 — SUA Address Mapping Rules

The following table explains the fields in this screen.

The fields in Menu 15.1.255 are read-only.

Table 6-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP Local End IP	**Local Start IP** is the starting local IP address (ILA) (see *Figure 6-1)*. **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	0.0.0.0 255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	N/A

Table 6-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Type	These are the mapping types discussed above (see *Table 6-2*). **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

User-Defined Address Mapping Sets

Now let’s look at Option 1 in menu 15.1. Enter 1 to bring up this menu. We’ll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set. If the **Set Name** field is left blank, the entire set will be deleted.

```
                        Menu 15.1.1 - Address Mapping Rules

 Set Name= NAT_SET

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.
 2
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                  Action= Edit          Select Rule=N/A

                  Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-8 Menu 15.1.1 — First Set

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

Ordering Your Rules

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 6-5 Fields in Menu 15.1.1

FIELD	DESCRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.	**Edit**
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An End IP address must be numerically greater than its corresponding IP Start address.

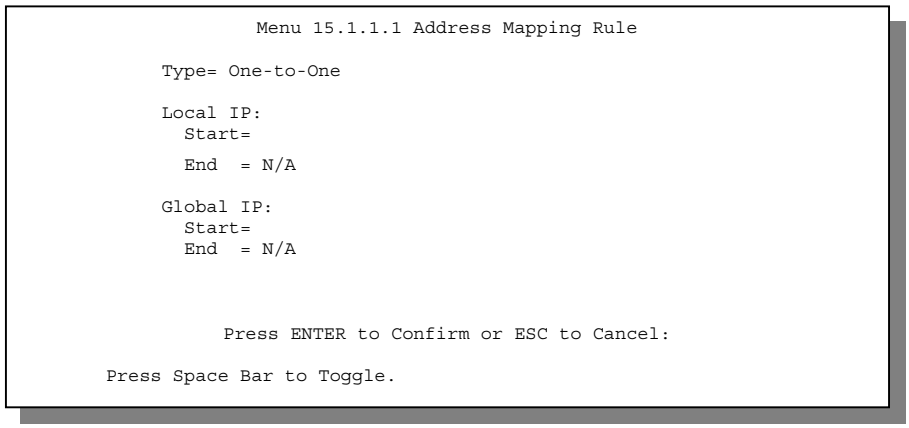


Figure 6-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

Table 6-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] to toggle through a total of five types. These are the mapping types discussed in Table 6-2. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 6.5.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

6.4 NAT Server Sets – Port Forwarding

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. Entry 12 (port 1026) is non-editable (see Figure 6-10).

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

The most often used port numbers are shown in the following table. Please refer to *RFC 1700* for further information about port numbers. Please also refer to the included disk for more examples and details on NAT.

Table 6-7 Services & Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53

Table 6-7 Services & Port Numbers

SERVICES	PORT NUMBER
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

6.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

Step 2. Enter 2 to go to **Menu 15.2 - NAT Server Setup**.

Step 3. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 4. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 5. Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

```
                    Menu 15.2 - NAT Server Setup


 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------------
   1.     Default          Default        0.0.0.0
   2.       21               25           192.168.1.33
   3.       0                0            0.0.0.0
   4.       0                0            0.0.0.0
   5.       0                0            0.0.0.0
   6.       0                0            0.0.0.0
   7.       0                0            0.0.0.0
   8.       0                0            0.0.0.0
   9.       0                0            0.0.0.0
  10.       0                0            0.0.0.0
  11.       0                0            0.0.0.0
  12.       1026             1026         RR Reserved

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-10 Menu 15.2 — NAT Server Setup

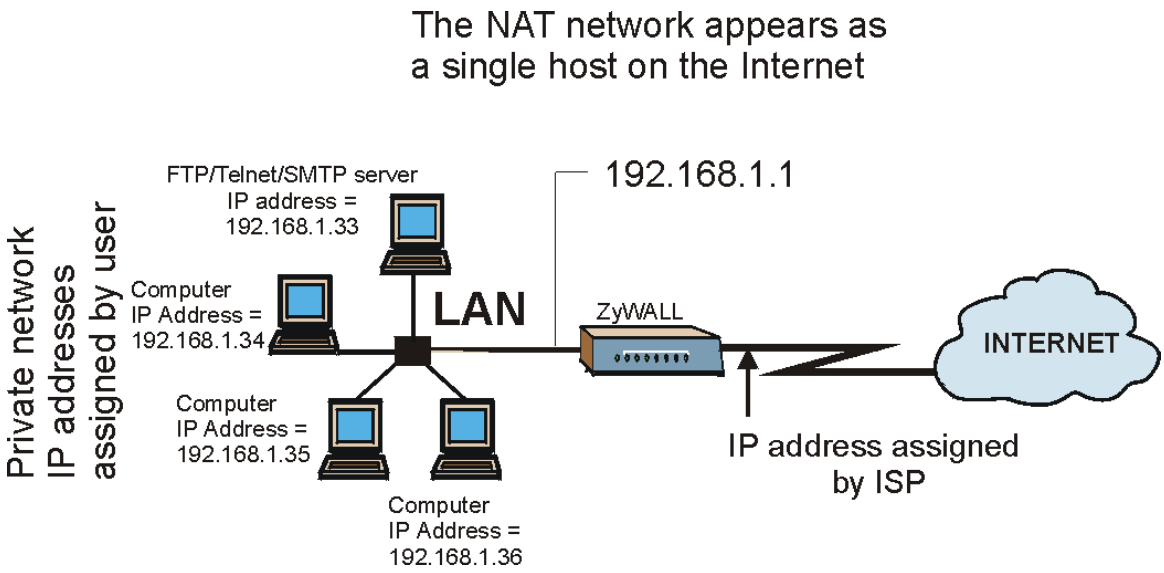


Figure 6-11 Multiple Servers Behind NAT Example

6.5 General NAT Examples

6.5.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

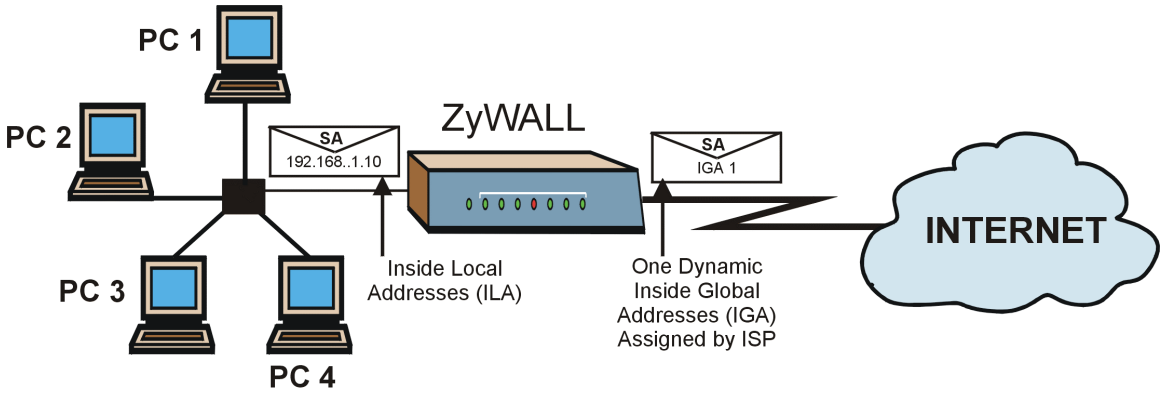


Figure 6-12 NAT Example 1

```
                Menu 4 - Internet Access Setup

        ISP's Name= ChangeMe
        Encapsulation= Ethernet
        Service Type= Standard
          My Login= N/A
          My Password= N/A
          Login Server IP= N/A

        IP Address Assignment= Dynamic
          IP Address= N/A
          IP Subnet Mask= N/A
          Gateway IP Address= N/A
        Network Address Translation= SUA Only




        Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-13 Menu 4 — Internet Access & NAT Example

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 6.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

6.5.2 Example 2: Internet Access with an Inside Server

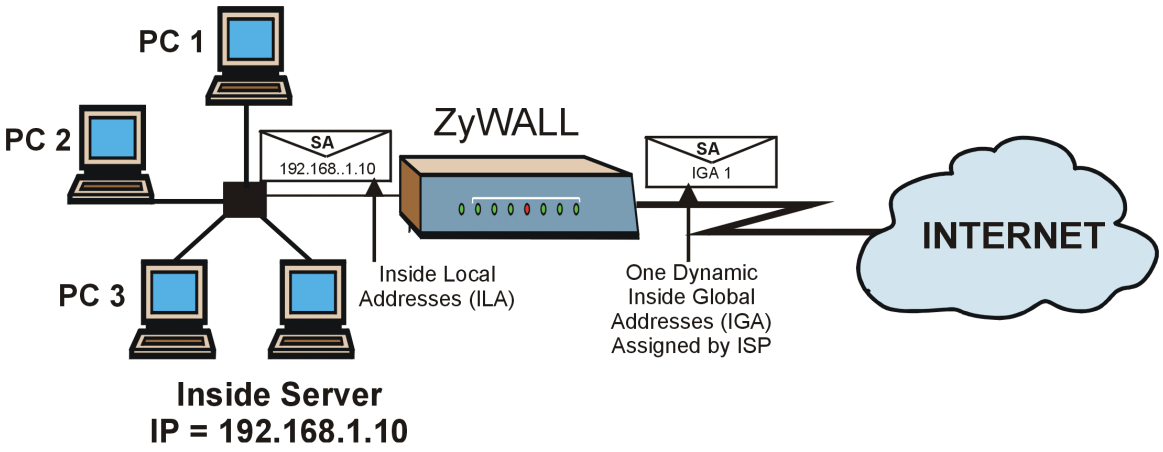


Figure 6-14 NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

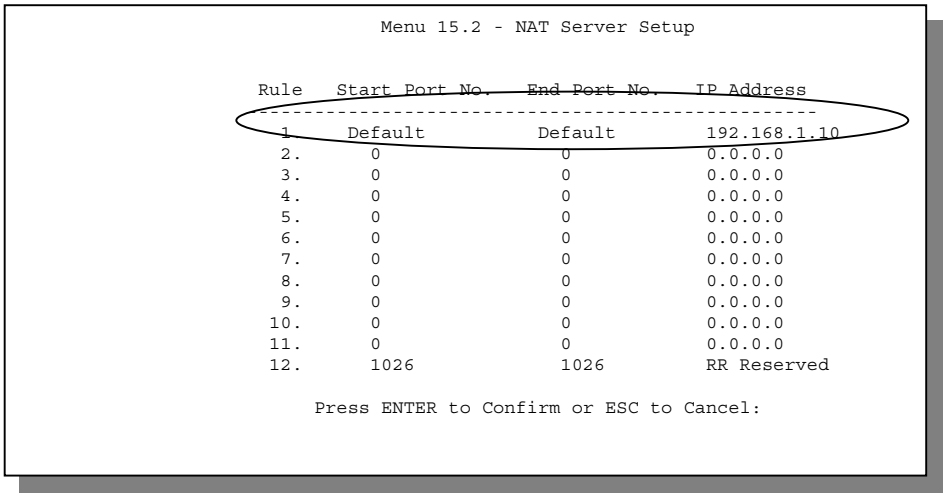

Menu 15.2 - NAT Server Setup
Rule Start Port No. End Port No. IP Address
1. Default Default 192.168.1.10
2. 0 0 0.0.0.0
3. 0 0 0.0.0.0
4. 0 0 0.0.0.0
5. 0 0 0.0.0.0
6. 0 0 0.0.0.0
7. 0 0 0.0.0.0
8. 0 0 0.0.0.0
9. 0 0 0.0.0.0
10. 0 0 0.0.0.0
11. 0 0 0.0.0.0
12. 1026 1026 RR Reserved
Press ENTER to Confirm or ESC to Cancel:

Figure 6-15 Menu 15.2 — Specifying an Inside Server

6.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

Rule 1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

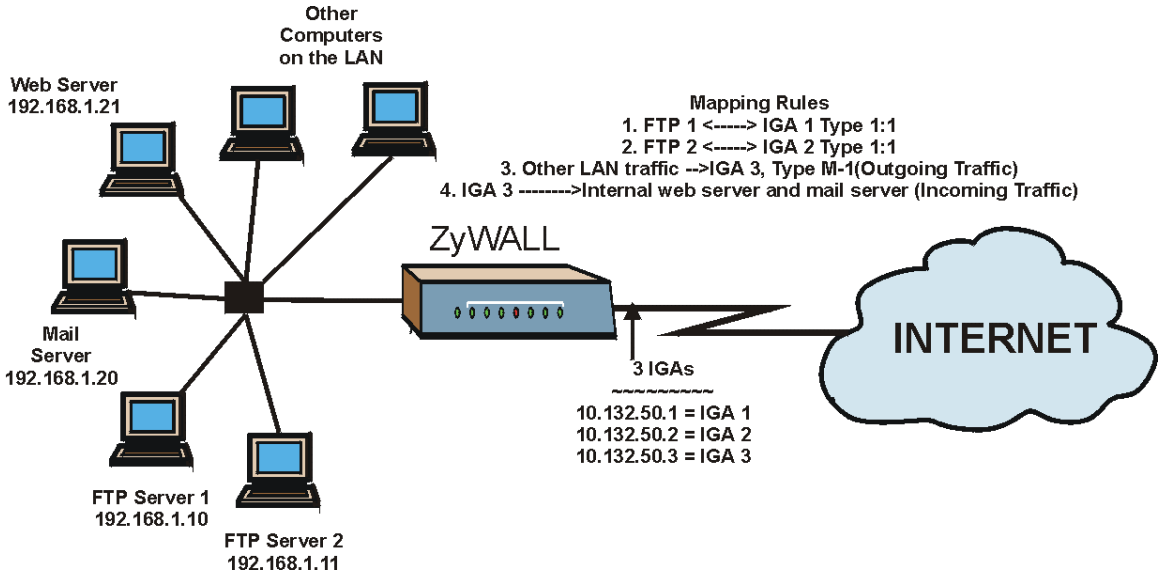


Figure 6-16 NAT Example 3

Step 1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 6-17.

Step 2. Then enter 15 from the main menu.

Step 3. Enter 1 to configure the Address Mapping Sets.

Step 4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 6-18).*

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

Step 7. When finished, menu 15.1.1 should look like as shown in *Figure 6-19.*

```
                Menu 11.3 - Remote Node Network Layer Options

          IP Address Assignment= Dynamic
          IP Address= N/A
          IP Subnet Mask= N/A
          Gateway IP Addr= N/A

          Network Address Translation= Full Feature
          Metric= N/A
          Private= N/A
          RIP Direction= None
          Version= N/A




          Enter here to CONFIRM or ESC to CANCEL:
```

Figure 6-17 Example 3: Menu 11.3

The following figure shows how to configure the first rule.

```
                  Menu 15.1.1.1 Address Mapping Rule

          Type= One-to-One

          Local IP:
            Start= 192.168.1.10
            End  = N/A

          Global IP:
            Start= 10.132.50.1
            End  = N/A



                          Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

Figure 6-18 Example 3: Menu 15.1.1.1

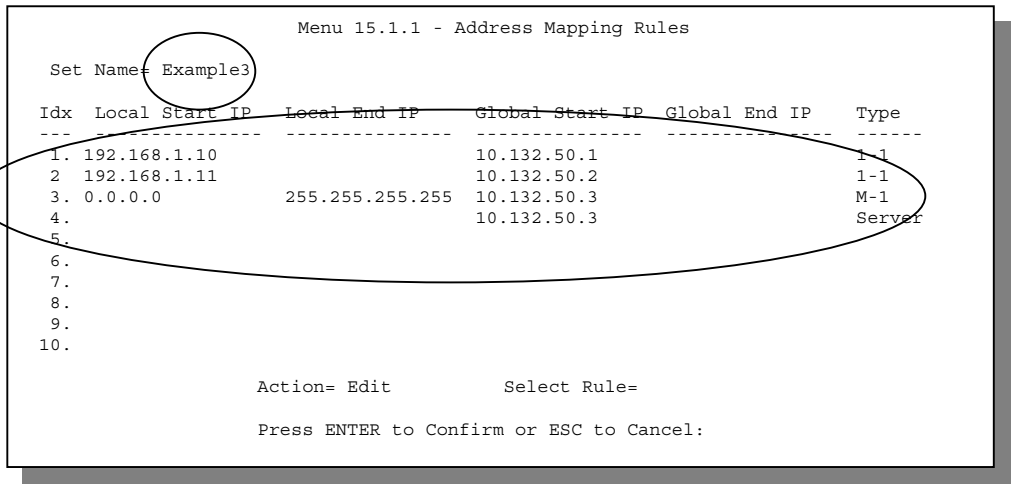


Figure 6-19 Example 3: Final Menu 15.1.1

Now configure the IGA3 to map to our web server and mail server on the LAN.

Step 8. Enter 15 from the main menu.

Step 9. Now enter 2 from this menu and configure it as shown in *Figure 6-20*.

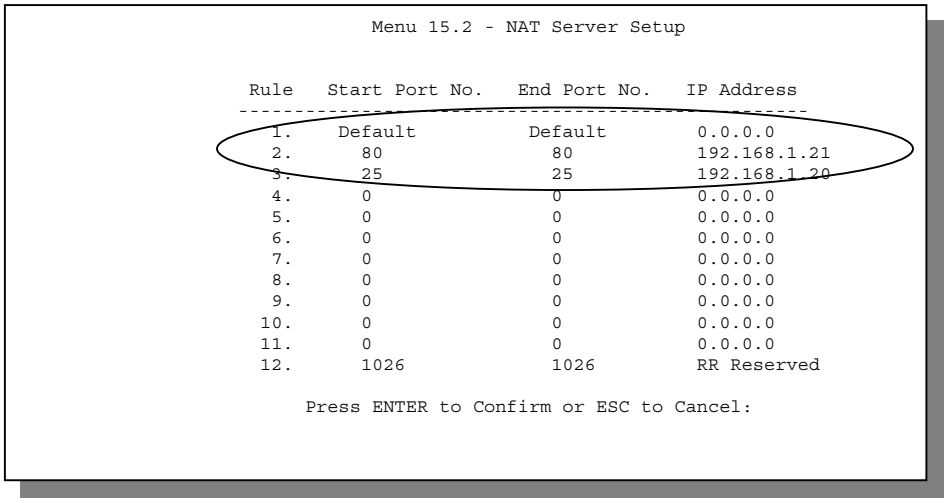

Menu 15.2 - NAT Server Setup
Rule Start Port No. End Port No. IP Address
1. Default Default 0.0.0.0
2. 80 80 192.168.1.21
3. 25 25 192.168.1.20
4. 0 0 0.0.0.0
5. 0 0 0.0.0.0
6. 0 0 0.0.0.0
7. 0 0 0.0.0.0
8. 0 0 0.0.0.0
9. 0 0 0.0.0.0
10. 0 0 0.0.0.0
11. 0 0 0.0.0.0
12. 1026 1026 RR Reserved
Press ENTER to Confirm or ESC to Cancel:

Figure 6-20 Example 3: Menu 15.2

6.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

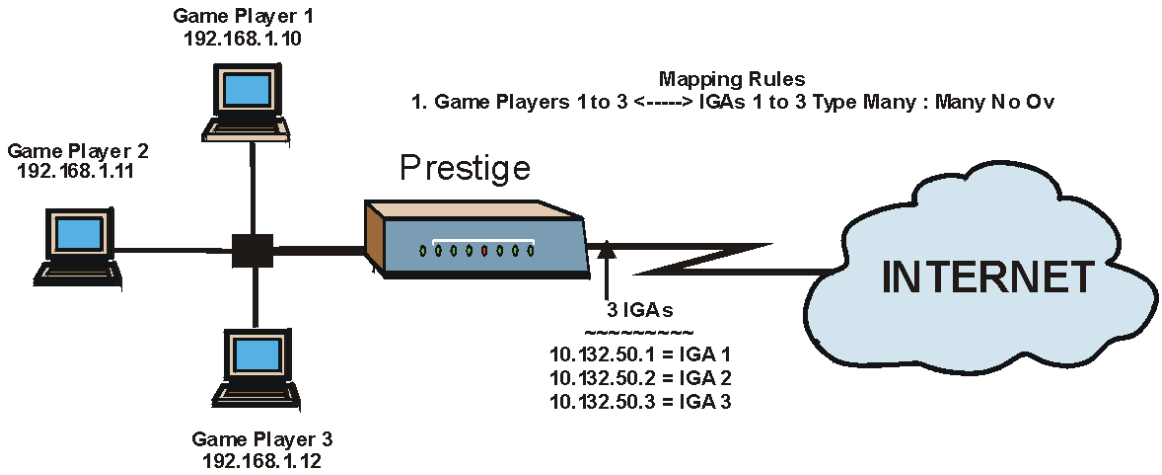


Figure 6-21 NAT Example 4

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One **and** Many-to-Many No Overload **mapping types.**

Follow the steps outlined in example 3 above to configure these two menus as follows.

```
                        Menu 15.1.1.1 Address Mapping Rule

          Type= Many-to-Many No Overload

          Local IP:
            Start= 192.168.1.10
            End  = 192.168.1.12

          Global IP:
            Start= 10.132.50.1
            End  = 10.132.50.3



                       Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```
                        Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M-M No Ov
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                   Action= Edit          Select Rule=

                   Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-23 Example 4: Menu 15.1.1 — Address Mapping Rules

Part III:

Firewall and Content Filters

Part III introduces firewalls in general and the ZyWALL firewall. It also explains custom ports and logs and gives example firewall rules and an overview of content filtering.

Chapter 7
Firewalls

This chapter gives some background information on firewalls and explains how to get started with the ZyWALL firewall.

7.1 What Is a Firewall?

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

7.2 Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

7.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

7.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

i. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

ii. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

7.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See *section 7.5* for more information on Stateful Inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

7.3 Introduction to ZyXEL's Firewall

The ZyWALL firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The ZyWALL's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyWALL can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyWALL also has packet filtering capabilities.

The ZyWALL is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyWALL has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into two areas.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless the remote host is authorized to use a specific service.

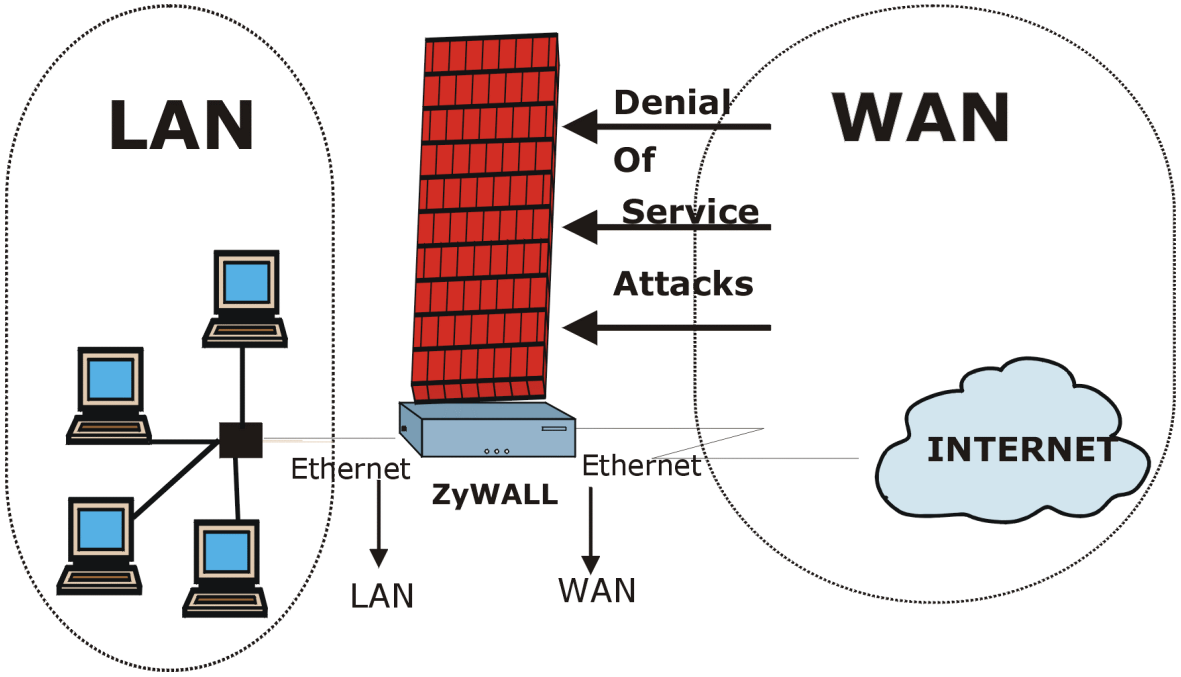


Figure 7-1 ZyWALL Firewall Application

7.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyWALL is pre-configured to automatically detect and thwart all known DoS attacks.

7.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. These protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc., are identified by an “extension number”, called the "TCP port" or "UDP port". For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended

for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 7-1 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

7.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.

1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

   1-a Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

   1-b Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

2. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

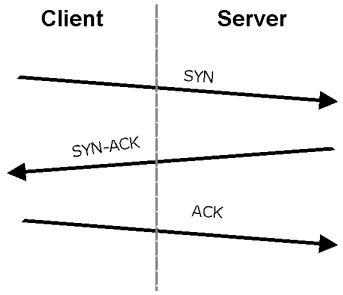


Figure 7-2 Three-Way Handshake

Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

2-a **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

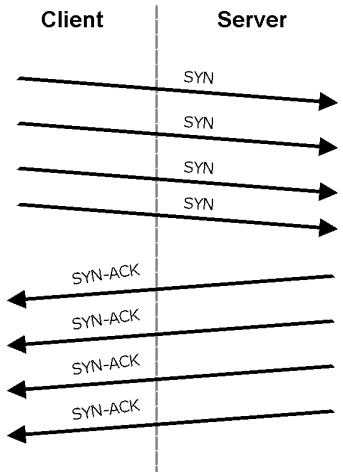


Figure 7-3 SYN Flood

2-b In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

3. A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

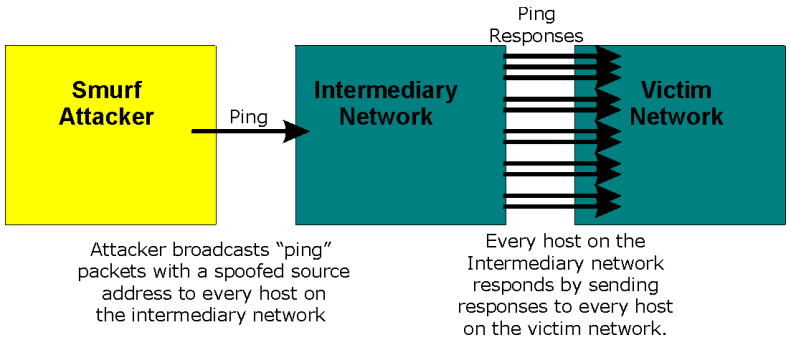


Figure 7-4 Smurf Attack

- ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 7-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 7-3 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 7-4 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

- Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

4. Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyWALL blocks all IP Spoofing attempts.

7.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This “remembering” is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyWALL uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyWALL’s stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).

- Denies all sessions originating from the WAN to the LAN.

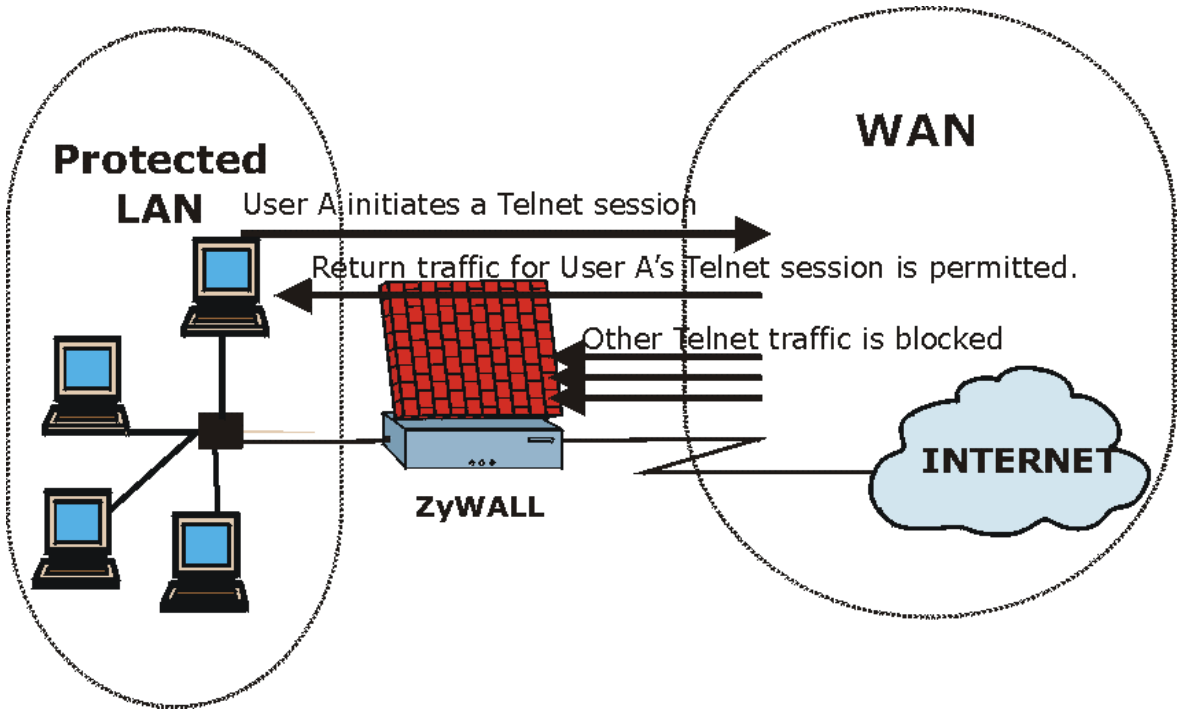


Figure 7-5 Stateful Inspection

The previous figure shows the ZyWALL's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

7.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).

3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **The default action for packets not matching following rules** field (see *Figure 10-3*) determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

7.5.2 Stateful Inspection and the ZyWALL

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

i. Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
ii. Allow certain types of traffic from the Internet to specific hosts on the LAN.
iii. Allow access to a Web server to everyone but competitors.
iv. Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic’s Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyWALL itself (as with the "virtual connections" created for UDP and ICMP).

7.5.3 TCP Security

The ZyWALL uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyWALL receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

7.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyWALL is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too

little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

7.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyWALL inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's Custom Ports feature to do this.

7.6 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via SMT or web configurator.
2. Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can telnet into your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

7.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

1. Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
2. DSL or cable modem connections are "always-on" connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
3. Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
4. Never e-mail sensitive information such as passwords, credit card information, etc.,without encrypting the information first.
5. Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
6. Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
7. Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
8. Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
9. If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers.
10. If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
11. Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

7.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyWALL's filtering and firewall functions.

7.7.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

When To Use Filtering

1. To block/allow LAN packets by their MAC address.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

7.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.

3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

Chapter 8
Introducing the ZyWALL Firewall

This chapter shows you how to get started with the ZyWALL firewall.

8.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management from the WAN, it overrides the firewall. See the *Remote Management* chapter for details.

8.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyWALL has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to the appendix of firewall CLI commands.

8.3 Using ZyWALL SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

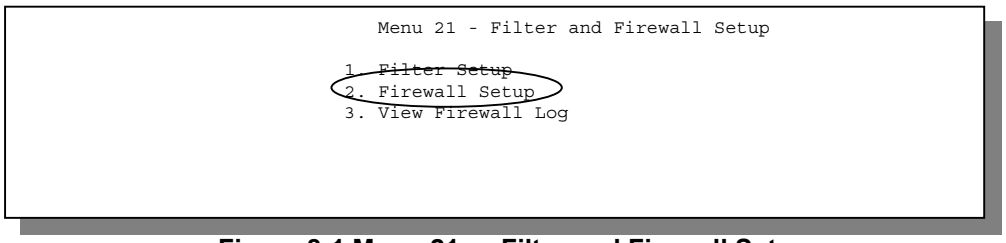


Figure 8-1 Menu 21 — Filter and Firewall Setup

8.3.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

```
                        Menu 21.2 - Firewall Setup

The firewall protects against Denial of Service (DOS) attacks when
it is active. The default Policy sets

    1. allow all sessions originating from the LAN to the WAN and
    2. deny all sessions originating from the WAN to the LAN

You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so

   Active: No

    LAN-to-WAN Set Name: ACL Default Set
    WAN-to-LAN Set Name: ACL Default Set

Please configure the Firewall function through ZyWALL Web Configurator.

              Press ENTER to Confirm or ESC to Cancel:
```

Figure 8-2 Menu 21.2 — Firewall Setup

Configure the firewall rules using the web configurator or CLI commands.

8.3.2 Viewing the Firewall Log

In menu 21, enter 3 to view the firewall log. An example of a firewall log is shown next.

```
# Time      Packet Information                  Reason            Action
0|Jan 1 00 |From:192.168.17.1 To:192.168.17.255 |default policy |block
  | 15:43:19|UDP src port:00520 dest port:00520  |<2,00>         |
1|Jan 1 00 |From:172.20.1.179 To:172.21.1.66    |default policy |block
  | 15:43:20|UDP src port:03571 dest port:00161  |<2,00>         |
2|Jan 1 00 |From:172.21.1.148 To:172.21.255.255 |default policy |block
  | 15:43:20|UDP src port:00137 dest port:00137  |<2,00>         |
Clear Firewall Log (y/n):
```

Figure 8-3 Example Firewall Log

An “End of Log” message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

Table 8-1 View Firewall Log

FIELD	DESCRIPTION	EXAMPLES
#	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will	23

Table 8-1 View Firewall Log

FIELD	DESCRIPTION	EXAMPLES
#	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	23
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real time; otherwise the clock will start at 2000/01/01 00:00:00 the last time the ZyWALL was reset.	mm:dd:yy e.g., Jan 1 00 hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as protocol and src/dest port numbers (TCP, UDP), or protocol, type and code (ICMP).	From and To IP addresses Protocol and port numbers
Reason	This field states the reason for the log; i.e., was the rule matched, not matched or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets;:set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule. This is a log for a DoS attack.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol. attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop or syn flood
Action	This field displays whether the packet was blocked or forwarded. None means that no action is dictated by this rule.	block, forward or none
After viewing the firewall log, ENTER “y” to clear the log or “n” to retain it. With either option you will be returned to **Menu 21- Filter and Firewall Setup**.		

Chapter 9
Using the ZyWALL Web Configurator

This chapter shows you how to configure your firewall with the web configurator.

9.1 Web Configurator Login and Main Menu Screens

Use the ZyWALL web configurator, to configure your firewall. To get started, follow the steps shown next.

Step 1. Launch your web browser and enter 192.168.1.1 as the URL.

Step 2. Enter "1234" (default) as the password and click **Login**. If a password appears automatically, just click **Login**. You should see a screen asking you to change your password (highly recommended).

Step 3. Either enter a new password (and retype it to confirm) and click **Login** or click **Ignore** to display the **MAIN MENU** screen as shown next.

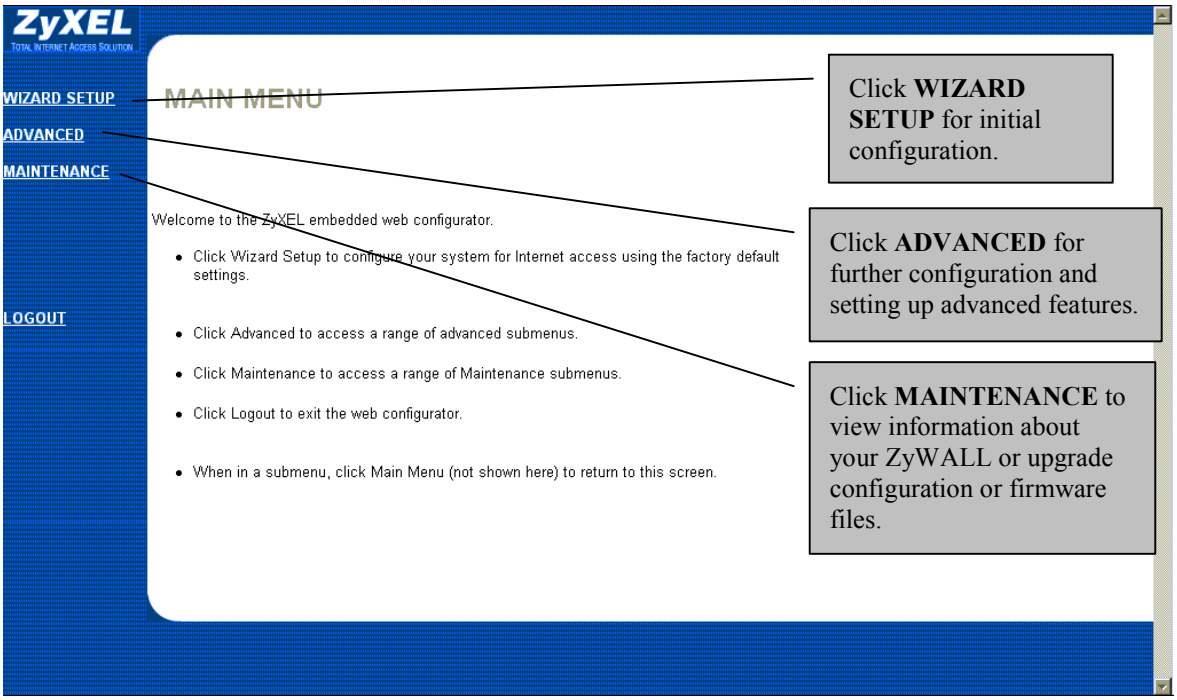

ZyXEL
TOTAL INTERNET ACCESS SOLUTION
WIZARD SETUP
ADVANCED
MAINTENANCE
LOGOUT
MAIN MENU
Welcome to the ZyXEL embedded web configurator.
Click Wizard Setup to configure your system for Internet access using the factory default settings.
Click Advanced to access a range of advanced submenus.
Click Maintenance to access a range of Maintenance submenus.
Click Logout to exit the web configurator.
When in a submenu, click Main Menu (not shown here) to return to this screen.
Click WIZARD SETUP for initial configuration.
Click ADVANCED for further configuration and setting up advanced features.
Click MAINTENANCE to view information about your ZyWALL or upgrade configuration or firmware files.

Figure 9-1 Main Menu

Use the HELP icon (located in the upper right portion of most screens) for online HTML help.

If you forget your password, refer to the *Resetting the ZyWALL* section to see how to reset the default configuration file.

9.2 Enabling the Firewall

Click **Advanced**, **Firewall**, **Configuration** and then the **Config** tab. Enable (or activate) the firewall by clicking the **Firewall Enabled** check box as seen in the following screen.

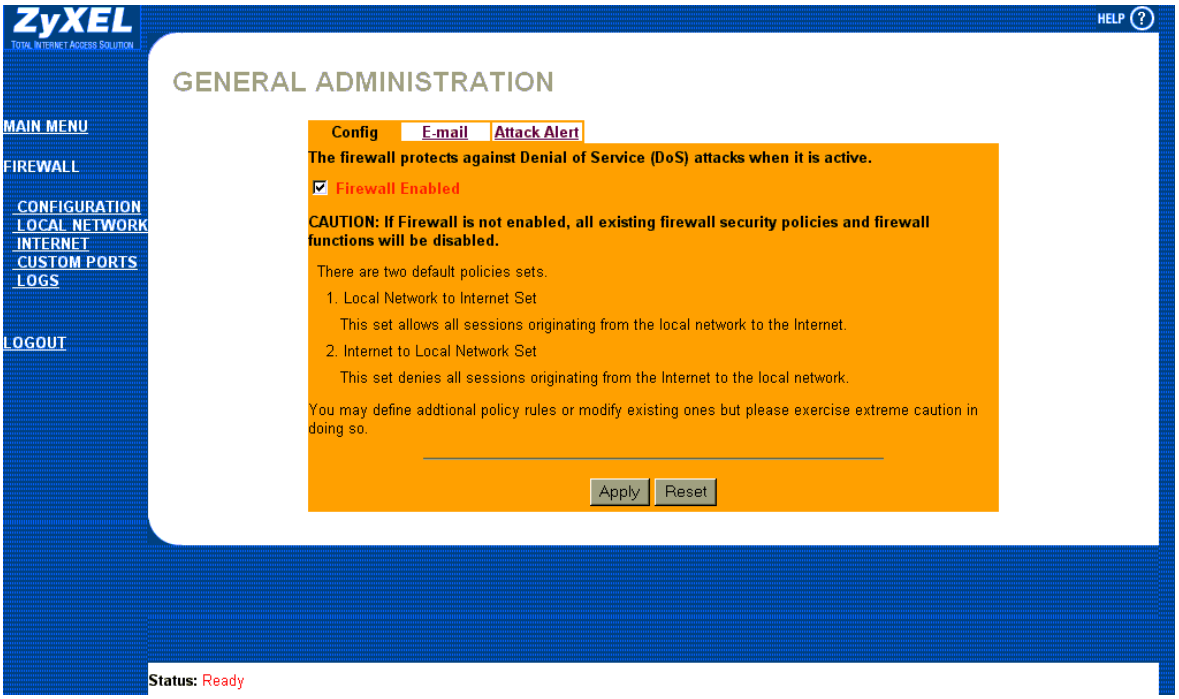

ZyXEL
TOTAL INTERNET ACCESS SOLUTION
HELP
GENERAL ADMINISTRATION
MAIN MENU
FIREWALL
CONFIGURATION
LOCAL NETWORK
INTERNET
CUSTOM PORTS
LOGS
LOGOUT
Config
E-mail
Attack Alert
The firewall protects against Denial of Service (DoS) attacks when it is active.
Firewall Enabled
CAUTION: If Firewall is not enabled, all existing firewall security policies and firewall functions will be disabled.
There are two default policies sets.
1. Local Network to Internet Set
This set allows all sessions originating from the local network to the Internet.
2. Internet to Local Network Set
This set denies all sessions originating from the Internet to the local network.
You may define addtional policy rules or modify existing ones but please exercise extreme caution in doing so.
Apply
Reset
Status: Ready

Figure 9-2 Enabling the Firewall

9.3 E-mail

The E-mail screen show next, allows you to specify your mail server, where e-mail alerts should be sent as well as when and how often they should be sent.

9.3.1 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen *(Figure 9-5* - check the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Rule Config** screen (see *Figure*

10-4). When an event generates an alert, a message is immediately sent to an e-mail account specified by you. Enter the complete e-mail address to which alert messages will be sent in the **E-mail Alerts To** field and schedule times for sending alerts in the **Log Timer** fields in the **E-mail** screen (following screen).

9.3.2 Logs

A log is a detailed record that you create for packets that either match a rule, don't match a rule or both when you are creating/editing a firewall rule (see *Figure 10-4)*. You can also choose not to create a log for a rule in this screen. An attack automatically generates a log.

Click **Advanced**, **Firewall**, **Configuration** and then the **E-mail** tab to bring up the following screen.

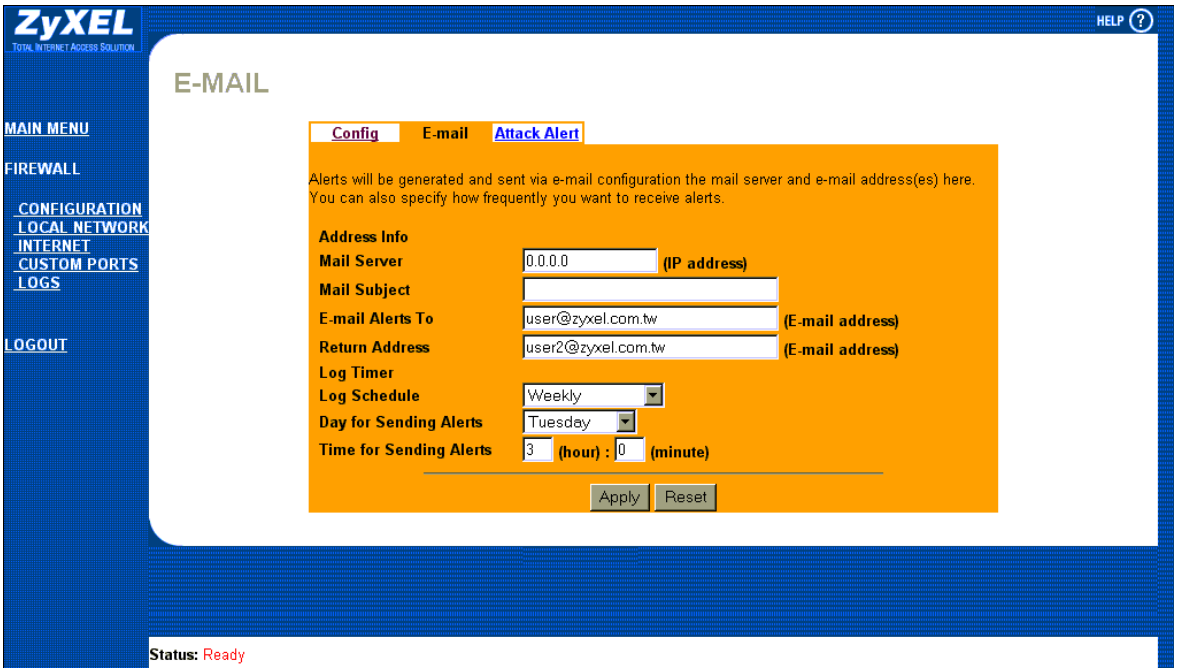


Figure 9-3 E-mail Screen

The following table describes the fields in this screen.

Table 9-1 E-mail

FIELD	DESCRIPTION	OPTIONS
Address Info		
Mail Server	Enter the IP address of your mail server in dotted decimal notation. Your Internet Service Provider (ISP) should be able to provide this information. If this field is left blank, log and alert messages will not be sent via e-mail.	
Mail Subject	Enter a subject that you want to appear in the subject field of your e-mail here (see *Figure 9-4)*. If you leave this field blank then the default "Firewall Alert From ZyWALL" displays as your e-mail subject.	
E-mail Alerts To	Enter the e-mail address (username@mydomain.com) of whoever is responsible for maintaining the firewall, e.g., your system administrator. If this field is left blank, alert messages will not be sent via e-mail.	
Return address	Enter an e-mail address to identify the ZyWALL as the sender of the e-mail messages i.e., a "return-to-sender" address for backup purposes.	
Log Timer		
Log Schedule	This pop-up menu is used to configure the frequency of log messages being sent as e-mail: daily, weekly, hourly, only when the log is full or none. If the **Weekly** or the **Daily** option is selected, specify a time of day when the e-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the e-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are e-mailed.	**When Log is Full** **Hourly** **Daily** **Weekly** **None**
Day for Sending Alerts	Click which day of the week you want to send the alert from the drop down list box.	**Sunday** through **Saturday**
Time for Sending Alerts	Click the up or down arrows to the right of the list box to choose a time to send the alerts.	
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

9.3.3 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear. Please see the *Support Notes* on the included disk for information on other types of error messages.

E-mail error messages appear in SMT menu 24.3.1 as "SMTP action request failed. ret= ??". The “??"are described in the following table.

Table 9-2 SMTP Error Messages

-1 means ZyWALL out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

9.3.4 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

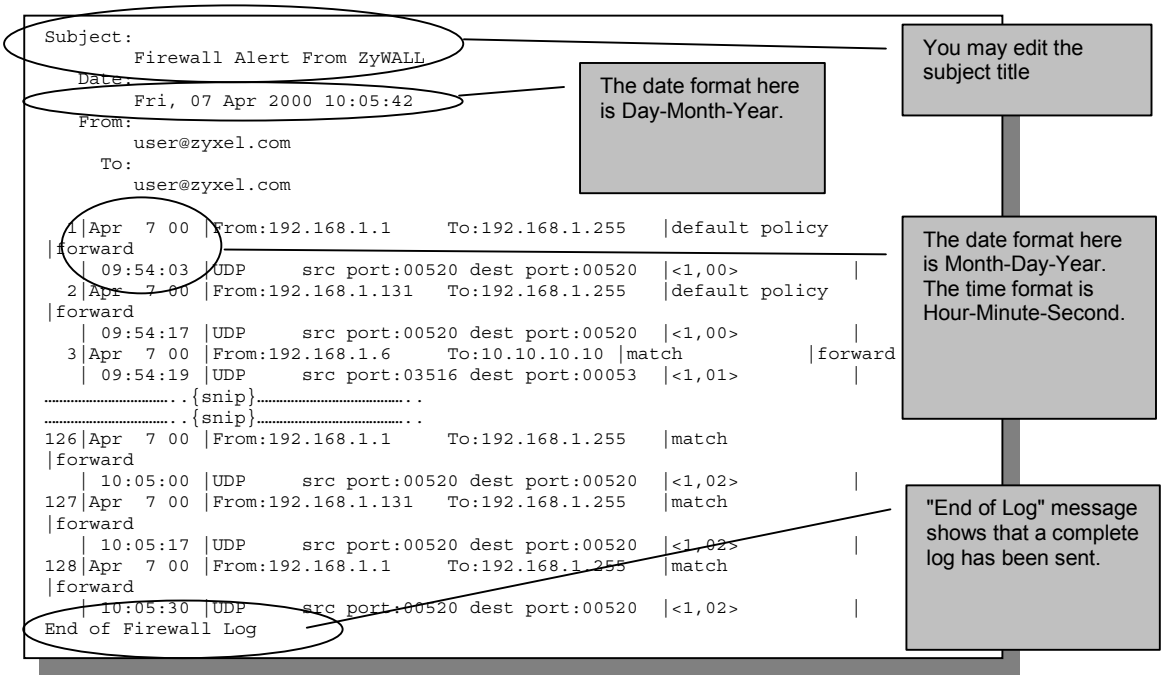

Subject:
Firewall Alert From ZyWALL
Date:
Fri, 07 Apr 2000 10:05:42
From:
user@zyxel.com
To:
user@zyxel.com
1|Apr 7 00 |From:192.168.1.1 To:192.168.1.255 |default policy
|forward
| 09:54:03 |UDP src port:00520 dest port:00520 |<1,00>
2|Apr 7 00 |From:192.168.1.131 To:192.168.1.255 |default policy
|forward
| 09:54:17 |UDP src port:00520 dest port:00520 |<1,00>
3|Apr 7 00 |From:192.168.1.6 To:10.10.10.10 |match |forward
| 09:54:19 |UDP src port:03516 dest port:00053 |<1,01>
{snip}
{snip}
126|Apr 7 00 |From:192.168.1.1 To:192.168.1.255 |match
|forward
| 10:05:00 |UDP src port:00520 dest port:00520 |<1,02>
127|Apr 7 00 |From:192.168.1.131 To:192.168.1.255 |match
|forward
| 10:05:17 |UDP src port:00520 dest port:00520 |<1,02>
128|Apr 7 00 |From:192.168.1.1 To:192.168.1.255 |match
|forward
| 10:05:30 |UDP src port:00520 dest port:00520 |<1,02>
End of Firewall Log
You may edit the subject title
The date format here is Day-Month-Year.
The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
"End of Log" message shows that a complete log has been sent.

Figure 9-4 E-mail Log

9.4 Attack Alert

Attack alerts are the first defense against DOS attacks. In the **Attack Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the ZyWALL uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

9.4.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for normal small offices with ADSL bandwidth. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.

2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.
You should make any changes to the threshold values before you continue configuring firewall rules.

9.4.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see *Figure 7-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

The ZyWALL measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the ZyWALL starts deleting half-open sessions as required to accommodate new connection requests. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the ZyWALL starts deleting half-open sessions as required to accommodate new connection requests. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the ZyWALL starts deleting half-open sessions according to one of the following methods:

1. If the **Blocking Time** timeout is 0 (the default), then the ZyWALL deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

2. If the **Blocking Time** timeout is greater than 0, then the ZyWALL blocks all new connection requests to the host giving the server time to handle the present connections. The ZyWALL continues to block all new connection requests until the **Blocking Time** expires.

The ZyWALL also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click on the **Attack Alert** tab to bring up the next screen.

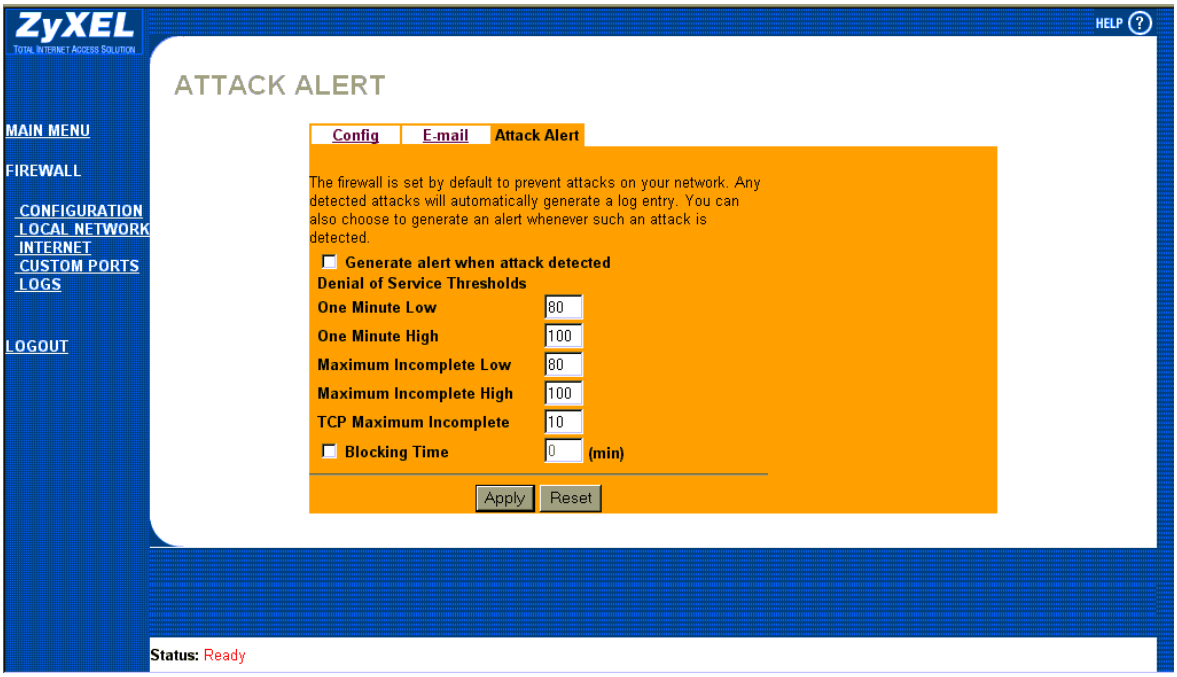


Figure 9-5 Attack Alert

The following table describes the fields in this screen.

Table 9-3 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected. See the *Logs Chapter* for more information on logs and alerts.	

Table 9-3 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyWALL to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number.	100 half-open sessions per minute. The above values causes the ZyWALL to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination	10 existing half-open TCP sessions.

Table 9-3 Attack Alert

FIELD	DESCRIPTION	DEFAULT VALUES
Incomplete	host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 250. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	sessions.
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you check **Blocking Time** any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	Select this check box to specify a number in minutes (min) text box.
(min)	Enter the length of **Blocking Time** in minutes.	0
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

Chapter 10
Creating Custom Rules

This chapter contains instructions for defining both Local Network and Internet rules.

10.1 Rules Overview

Firewall rules are subdivided into "Local Network" and "Internet". By default, the ZyWALL's stateful packet inspection allows all communications to the Internet that originate from the local network, and blocks all traffic to the LAN that originates from the Internet. You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

If you try to configure rules but do not have a good understanding of how rules work, you might inadvertently introduce security risks to the firewall and to the protected network. You should be sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing network traffic's Source IP address, Destination IP address, IP protocol type to rules set by the administrator. Your customized rules take precedence, and may override the ZyWALL's default rules.

10.2 Rule Logic Overview

Study these points carefully before configuring rules.

10.2.1 Rule Checklist

1. State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."

2. Is the intent of the rule to forward or block traffic?
3. What is the direction connection: from the LAN to the Internet, or from the Internet to the LAN?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

10.2.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the **Rules** screen in the web configurator.

10.2.3 Key Fields For Configuring Rules

Action

Should the action be to **Block** or **Forward**?

"Block" means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 10.5* for more information on predefined services.

Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

10.3 Connection Direction

This section talks about configuring firewall rules for connections going from LAN to WAN and WAN to LAN in your firewall.

10.3.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure Policy -> LAN to WAN -> Rules, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

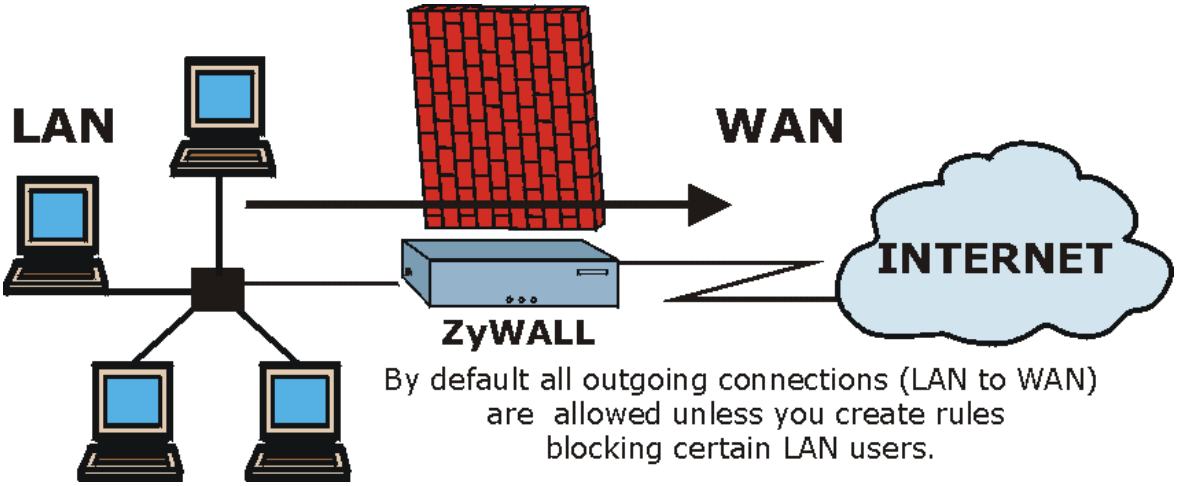


Figure 10-1 LAN to WAN Traffic

10.3.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

See the following figure.

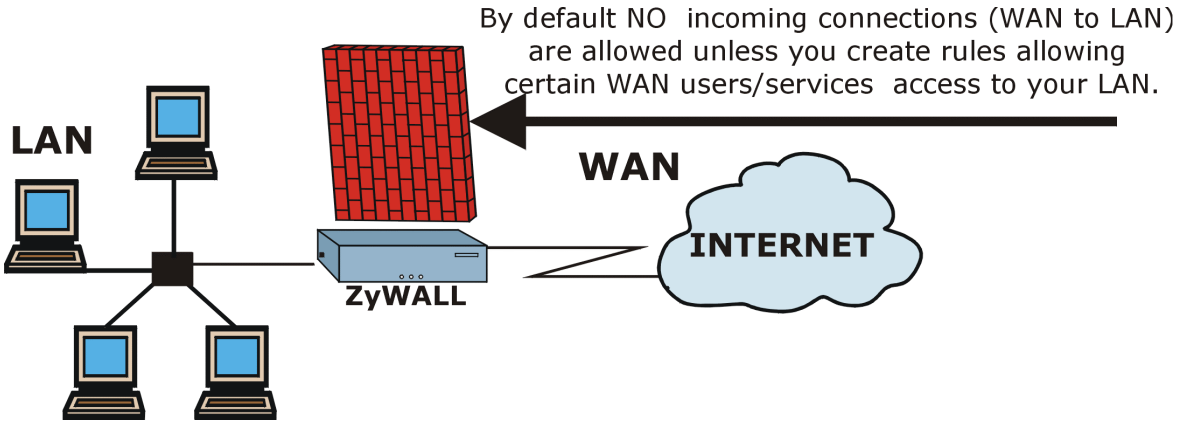


Figure 10-2 WAN to LAN Traffic

10.4 Rule Summary

The fields in the Rule Summary **screens are the same for** Local Network **and** Internet**, so the discussion below refers to both.**

Click on **Firewall**, then **Local Network** to bring up the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

The ordering of your rules is very important as rules are applied in turn.

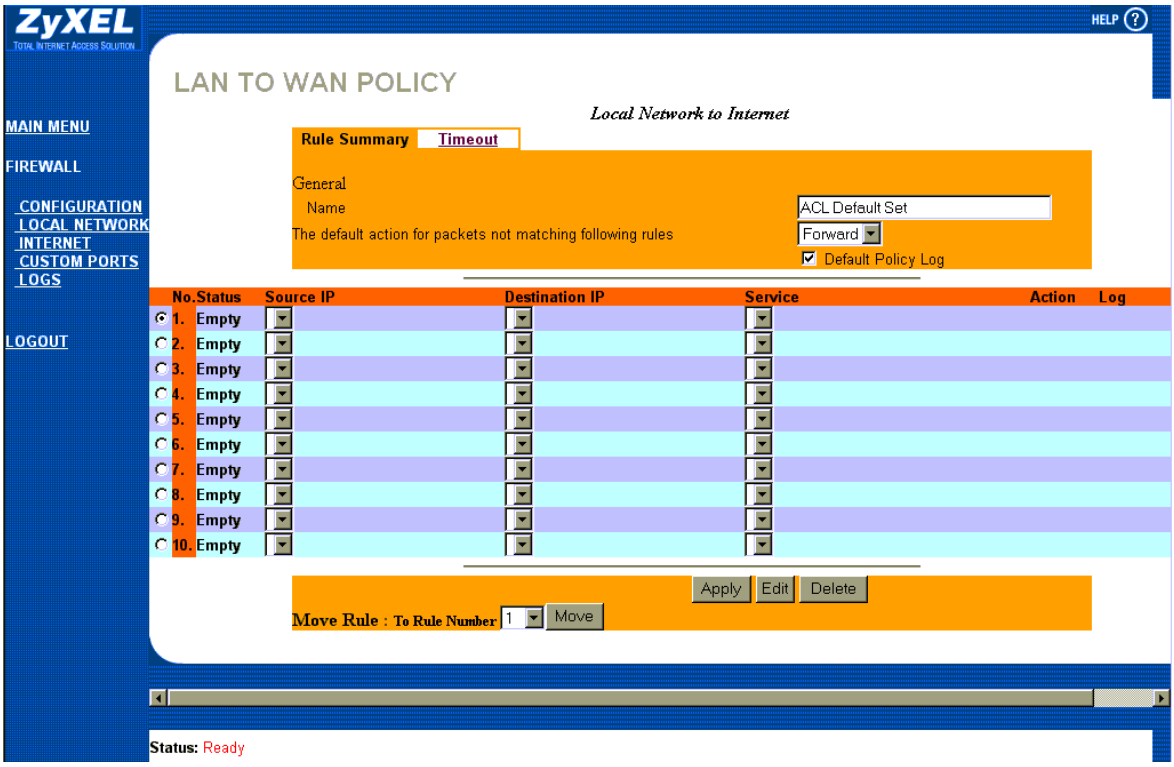


Figure 10-3 Firewall Rules Summary — First Screen

The following table describes the fields in this screen.

Table 10-1 Firewall Rules Summary — First Screen

FIELD	DESCRIPTION	OPTIONS
General Name	This is the name of the firewall rule set. Type a name to distinguish the LAN-to-WAN filter set from the WAN-to-LAN filter set.	Name
The default action for packets not matching following rules	Should packets that do not match the following rules be blocked or forwarded? Make your choice from the drop down list box. Note that “block” means the firewall silently discards the packet.	**Block** **Forward**

Table 10-1 Firewall Rules Summary — First Screen

FIELD	DESCRIPTION	OPTIONS
Default Policy Log	Click this check box to log all matched rules in the ACL default set.	
The following fields summarize the rules you have created. Note that these fields are read only. Click the tab at the top of the box to order the rules according to that tab.		
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules.	
Status	This field shows whether an individual rule has already been **Configured** or is still **Empty**.	**Empty** **Configured**
Source IP	This is the source address of the packet.	
Destination IP	This is the destination address of the packet.	
Service	This is the service to which the rule applies. See *Table 10-2* for more information.	
Action	This is the specified action for that rule. Note that **Block** means the firewall silently discards the packet.	**Block** **Forward**
Log	This field shows you if a log is created for packets that match the rule, don't match the rule, both or no log is created.	**Match** **Not Match** **Both** **None**
Alert	Scroll right to see the **Alert** field. This field shows you if an alert is generated when this rule is matched.	**Yes** **No**
Move Rule	You may reorder your rules using this function. Select by clicking on the rule you want to move. The ordering of your rules is important as rules are applied in turn.	
To Rule Number	Select the number you want to move the rule to.	
Move	Click **Move** to move the rule.	
Click **Apply** to create a new firewall rule. New firewall rules are added at the end after existing firewall rules. Click **Edit** to edit an existing filter rule. See *section 10.5* for more details. Click **Delete** to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action. Click **Help** for online HTML help on fields in this screen		

10.5 Predefined Services

The **Available Services** list box in the **Rule Config**(uration) screen (see *Figure 10-4*) displays all predefined services that the ZyWALL already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 10-2 Predefined Services

SERVICE	DESCRIPTION
AIM(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICMP	ICMP service allows normal ICMP packets to go through.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(ESP:0)	This service is used by the IPSec ESP (Encapsulation Security Protocol) tunneling protocol.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.

Table 10-2 Predefined Services

SERVICE	DESCRIPTION
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.

Table 10-2 Predefined Services

SERVICE	DESCRIPTION
STRM WORKS(UDP:1558)	Stream Works Protocol.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

10.5.1 Creating/Editing Firewall Rules

To create a new rule, click a number (**No.**) then click **Edit** in the last screen shown to display the following screen.

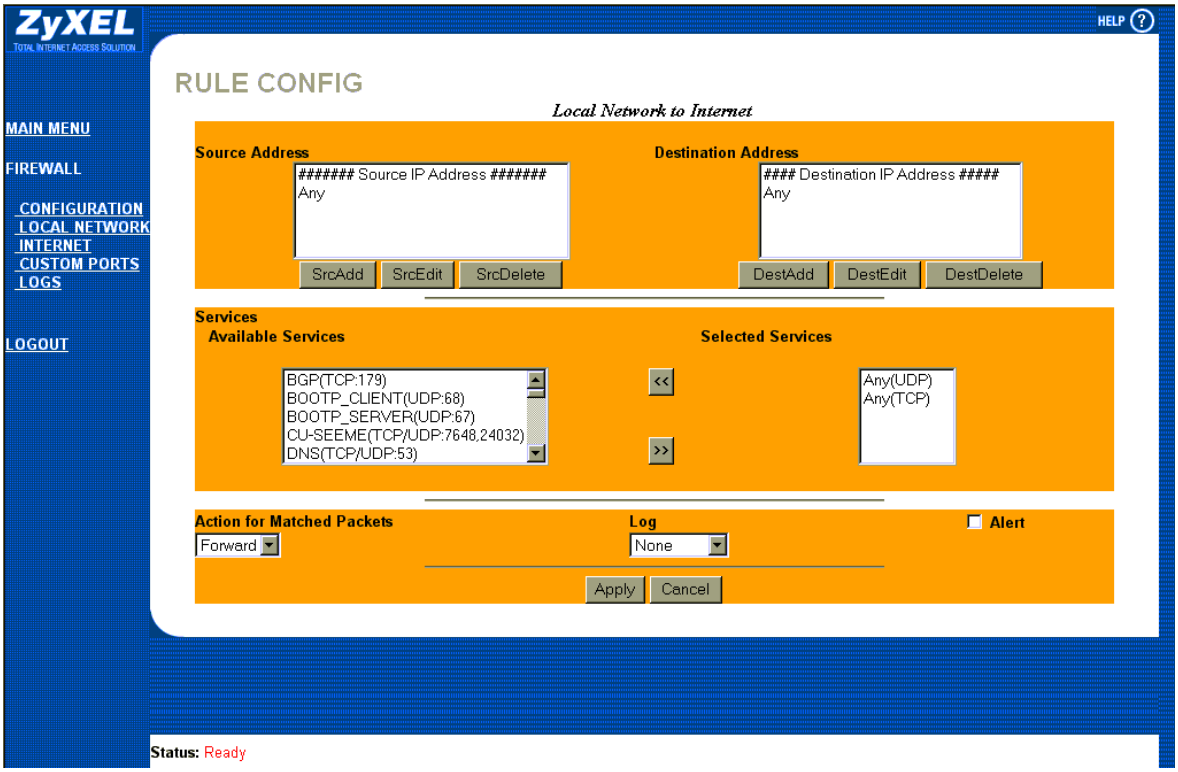


Figure 10-4 Creating/Editing A Firewall Rule

Table 10-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	OPTIONS
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one. Please see the next section for more information on adding and editing source addresses.	**SrcAdd** **SrcEdit** **SrcDelete**
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one.	**DestAdd**

Table 10-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	OPTIONS
	Please see the following section on adding and editing destination addresses.	**DestEdit** **DestDelete**
Services Available/Selected Services	Please see *Table 10-2* for more information on services available. Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **<<**.	**>>** **<<**
Action for Matched Packets	Should packets that match this rule be blocked or forwarded? Make your choice from the drop down list box. Note that **Block** means the firewall silently discards the packet.	**Block** **Forward**
Log	This field determines if a log is created for packets that match the rule, don't match the rule, both or no log is created.	**Match** **Not Match** **Both** **None**
Alert	Check the **Alert** check box to determine that this rule generates an alert when the rule is matched.	
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

10.5.2 Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen**.** Either action displays the following screen.

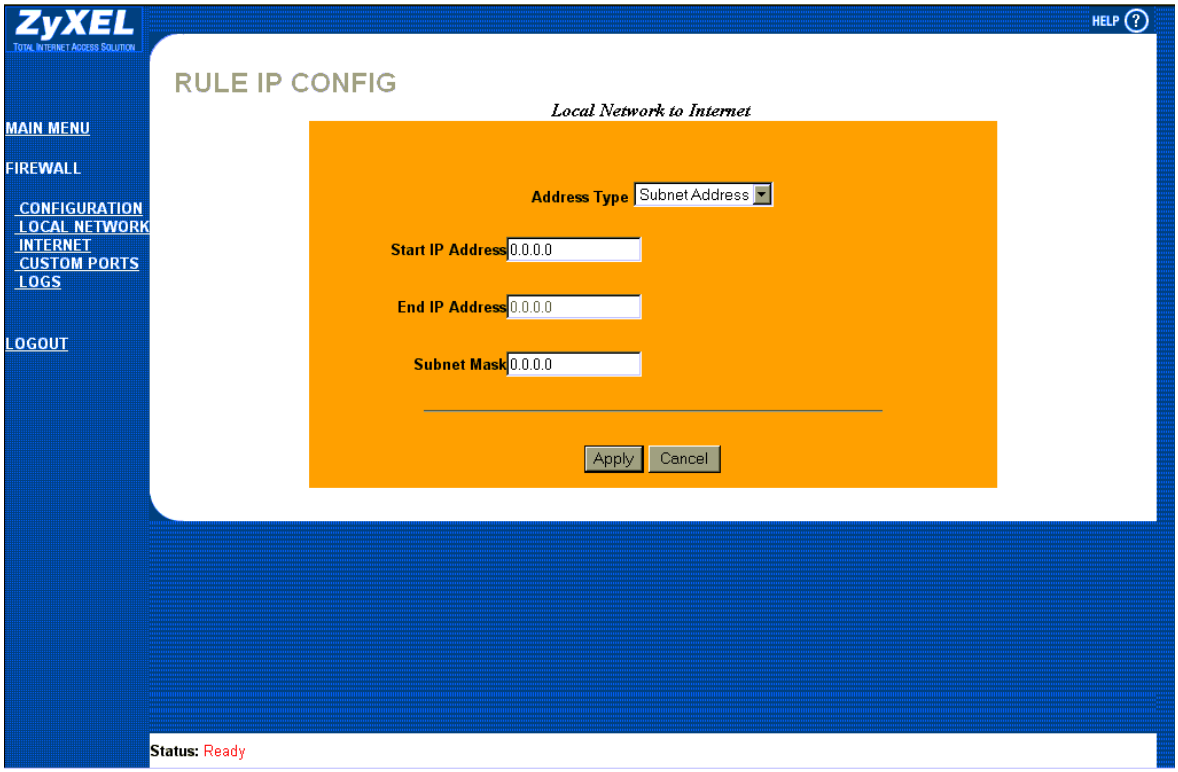


Figure 10-5 Adding/Editing Source and Destination Addresses

Table 10-4 Adding/Editing Source and Destination Addresses

FIELD	DESCRIPTION	OPTIONS
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop down list box	**Single Address** **Range Address** **Subnet Address** **Any Address**
Start IP Address	Enter the single IP address or the starting IP address in a range here.	
End IP Address	Enter the ending IP address in a range here.	
Subnet Mask	Enter the subnet mask here, if applicable.	
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

10.6 Timeout

The fields in the Timeout **screens are the same for** Local **and** Internet networks**, so the discussion below refers to both.**

10.6.1 Factors Influencing Choices for Timeout Values

The factors influencing choices for timeout values are the same as the factors influencing choices for threshold values – see *section 9.4.1.* Click on either **Local Network** or **Internet**, then select the **Timeout** tab.

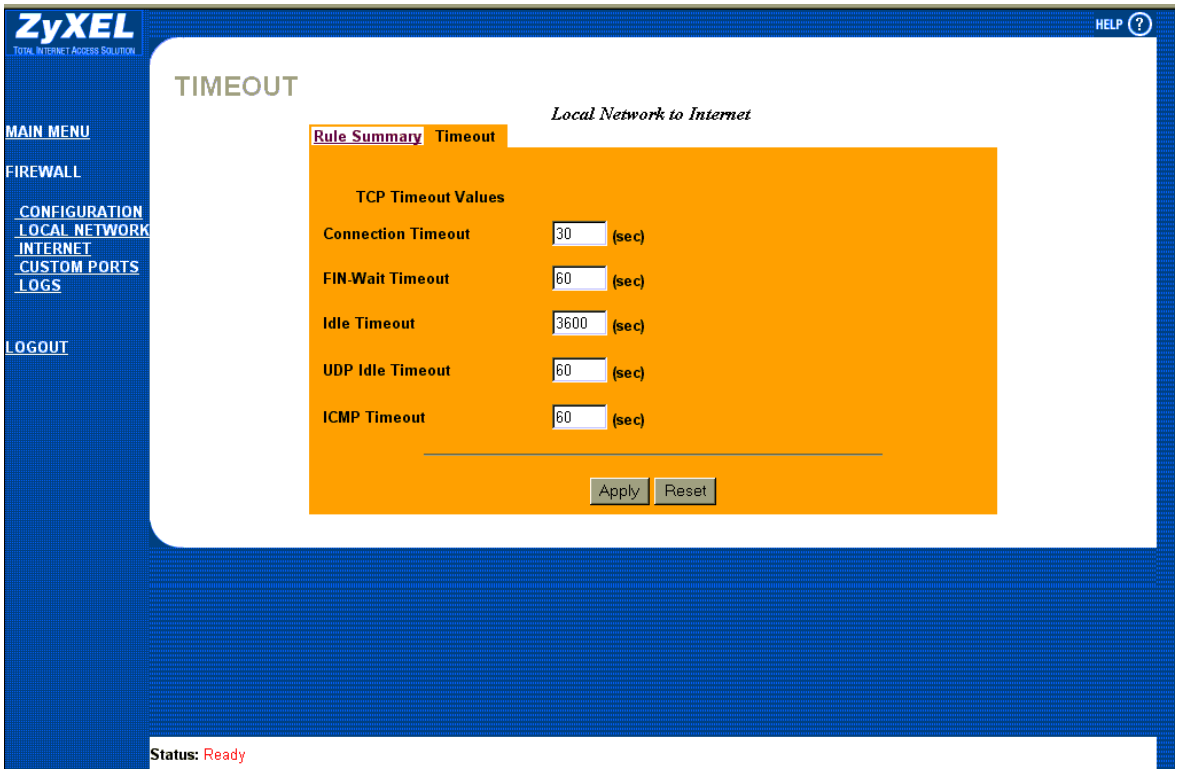


Figure 10-6 Timeout Screen

Table 10-5 Timeout Menu

FIELD	DESCRIPTION	DEFAULT VALUE
TCP Timeout Values		
Connection Timeout	This is the length of time the ZyWALL waits for a TCP session to reach the established state before dropping the session.	30 seconds
FIN-Wait Timeout	This is the length of time a TCP session remains open after the firewall detects a FIN-exchange (indicating the end of the TCP session).	60 seconds
Idle Timeout	This is the length of time of inactivity a TCP connection remains open before the ZyWALL considers the connection closed.	3600 seconds (1 hour)
UDP Idle Timeout	This is the length of time of inactivity a UDP connection remains open before the ZyWALL considers the connection closed.	60 seconds
ICMP Timeout	This is the length of time an ICMP session waits for the ICMP response.	60 seconds
When you have finished, click on **Apply** to apply your changes or **Reset** to go back to the original settings. Click **Help** for online HTML help on fields in this screen.		

Chapter 11
Custom Ports

This chapter covers creating, viewing and editing custom ports.

11.1 Introduction

Configure customized ports for services not predefined by the ZyWALL (see *Figure 10-4)*. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read *section 10.5*. To configure a custom port, click **Custom Ports** to bring up the following screen.

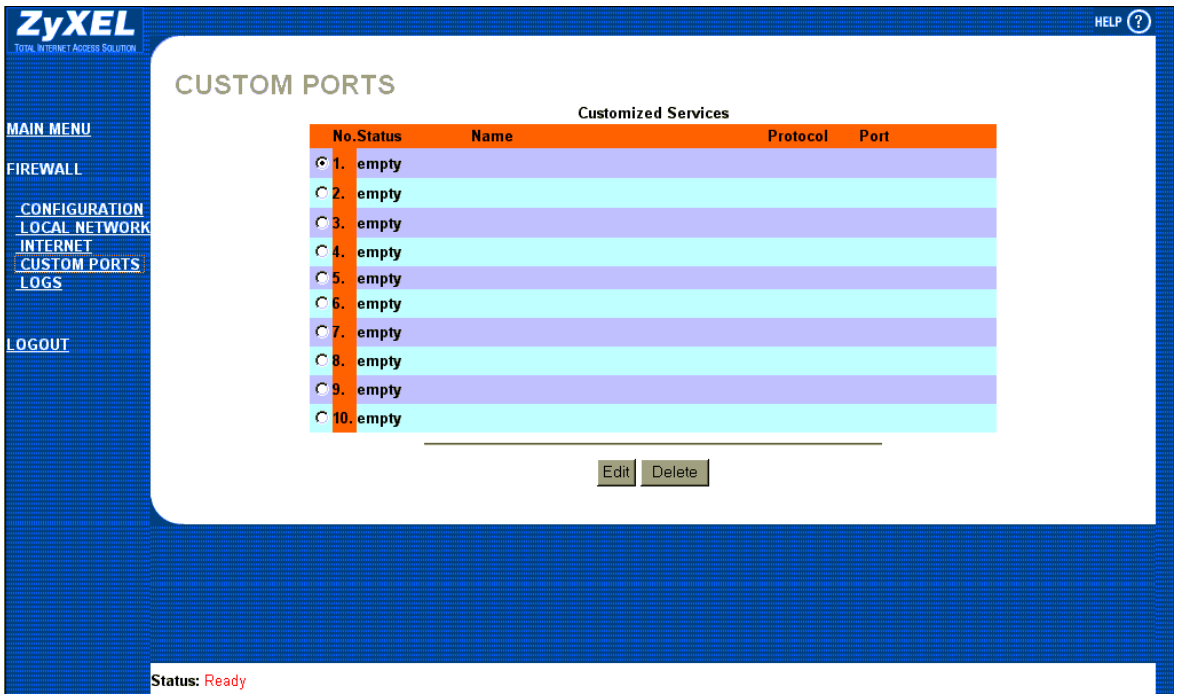


Figure 11-1 Custom Ports

The next table describes the fields in this screen.

Table 11-1 Custom Ports

FIELD	DESCRIPTION
Customized Services	
No.	This is the number of your customized port.
Status	Indicates whether ports have already been configured or are still empty.
Name	This is the name of your customized port.
Protocol	This shows the IP protocol (TCP, UDP or Both) that defines your customized port.
Port	This is the port number or range that defines your customized port.
Click a custom port number option box (No.) and then click **Edit** to edit an existing service (custom port) or **Delete** to delete that service (custom port). Click **Help** for online HTML help on fields in this screen. When you have finished viewing this screen, click another link to exit.	

11.2 Creating/Editing A Custom Port

Click **Edit** in the previous screen to create a new custom port or edit an existing one. This action displays the following screen.

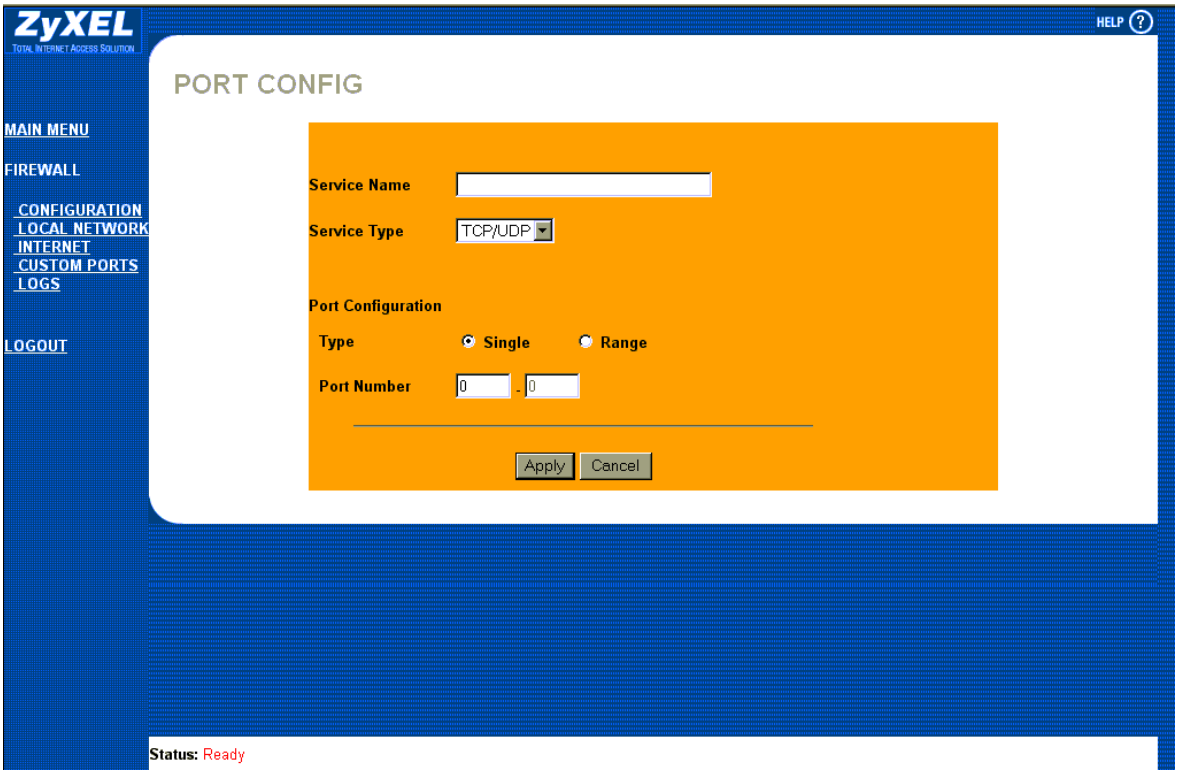


Figure 11-2 Creating/Editing A Custom Port

The next table describes the fields in this screen.

Table 11-2 Creating/Editing A Custom Port

FIELD	DESCRIPTION	OPTIONS
Service Name	Enter a unique name for your custom port.	
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized port from the drop down list box.	**TCP** **UDP** **Both**
Port Configuration Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.	**Single** **Range**
Port Number	Enter a single port number or the range of port numbers that define your customized service.	
When you have finished, click **Apply** to save your customized settings and exit this screen, **Cancel** to exit this screen without saving, or **Help** for online HTML help on fields in this screen.		

Chapter 12
Logs

This chapter contains information about using the log screen to view the results of the rules you have configured.

12.1 Log Screen

When you configure a new rule you also have the option to log events that match, don't match (or both) this rule (see *Figure 10-4*). Click on the **Logs** to bring up the next screen. Firewall logs may also be viewed in SMT Menu 21.3 (see *section 8.3)* or via syslog (SMT **Menu 24.3.2 - System Maintenance - UNIX Syslog**). Syslog is an industry standard protocol used for capturing log information for devices on a network. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.

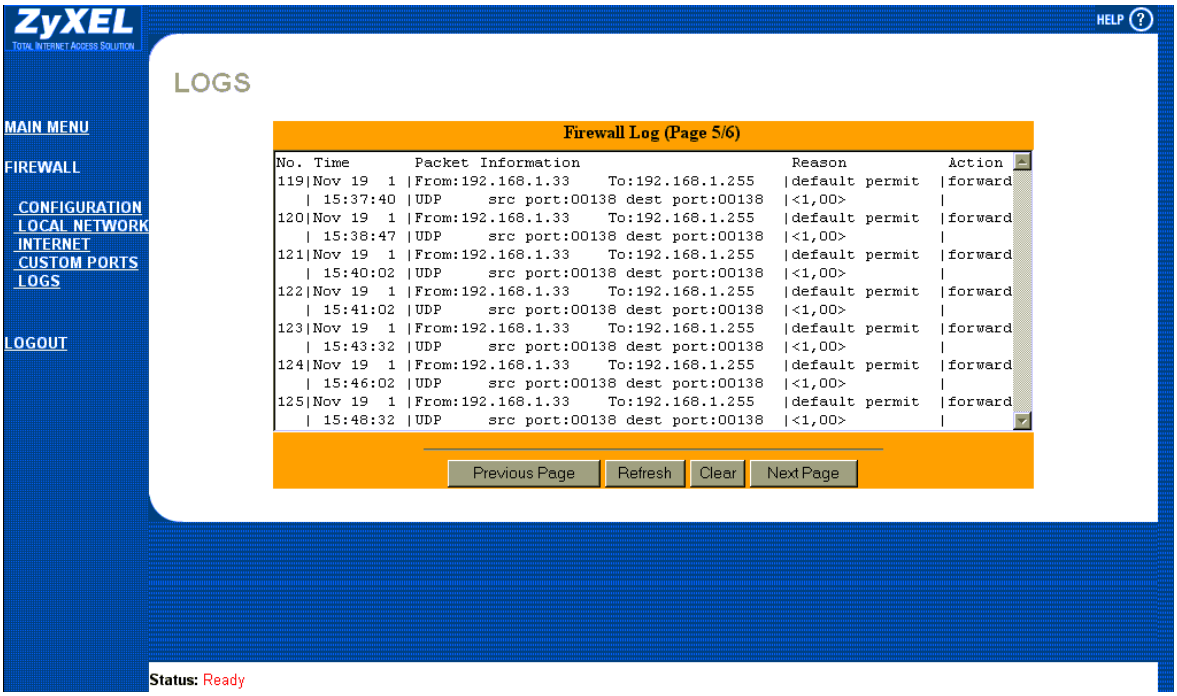

ZyXEL
TOTAL INTERNET ACCESS SOLUTION
HELP
LOGS
MAIN MENU
FIREWALL
CONFIGURATION
LOCAL NETWORK
INTERNET
CUSTOM PORTS
LOGS
LOGOUT
Firewall Log (Page 5/6)
No. Time Packet Information Reason Action
119|Nov 19 1 |From:192.168.1.33 To:192.168.1.255 |default permit |forward
| 15:37:40 |UDP src port:00138 dest port:00138 |<1,00> |
120|Nov 19 1 |From:192.168.1.33 To:192.168.1.255 |default permit |forward
| 15:38:47 |UDP src port:00138 dest port:00138 |<1,00> |
121|Nov 19 1 |From:192.168.1.33 To:192.168.1.255 |default permit |forward
| 15:40:02 |UDP src port:00138 dest port:00138 |<1,00> |
122|Nov 19 1 |From:192.168.1.33 To:192.168.1.255 |default permit |forward
| 15:41:02 |UDP src port:00138 dest port:00138 |<1,00> |
123|Nov 19 1 |From:192.168.1.33 To:192.168.1.255 |default permit |forward
| 15:43:32 |UDP src port:00138 dest port:00138 |<1,00> |
124|Nov 19 1 |From:192.168.1.33 To:192.168.1.255 |default permit |forward
| 15:46:02 |UDP src port:00138 dest port:00138 |<1,00> |
125|Nov 19 1 |From:192.168.1.33 To:192.168.1.255 |default permit |forward
| 15:48:32 |UDP src port:00138 dest port:00138 |<1,00> |
Previous Page
Refresh
Clear
Next Page
Status: Ready

Figure 12-1 Log Screen

Table 12-1 Log Screen

FIELD	DESCRIPTION	EXAMPLES
No.	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real-time; otherwise the time shown in these examples is displayed.	dd:mm:yy e.g., Jan 1 0 hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as:	From and To IP addresses protocol and port numbers.
Reason	This field states the reason for the log; i.e., was the rule matched, not matched, or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.	not match <1,01> dest IP This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
	This is a log for a DoS attack	attack land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop, or syn flood. *Chapter 7* has more detailed discussion of what these attacks mean.
Action	This field displays whether the packet was blocked (i.e., silently discarded), forwarded or neither (Block, Forward or None). “None” means that no action is dictated by this rule.	**Block**, **Forward** or **None**
Click **Previous Page** or **Next Page** to view other pages in your log. Click **Refresh** to renew the log screen or **Clear** to clear all the logs. Click **Help** for online HTML help on fields in this screen. When you have finished viewing this screen, click another link to exit.		

Chapter 13
Example Firewall Rules

This chapter gives examples for configuring various rules for WAN to LAN and LAN to WAN.

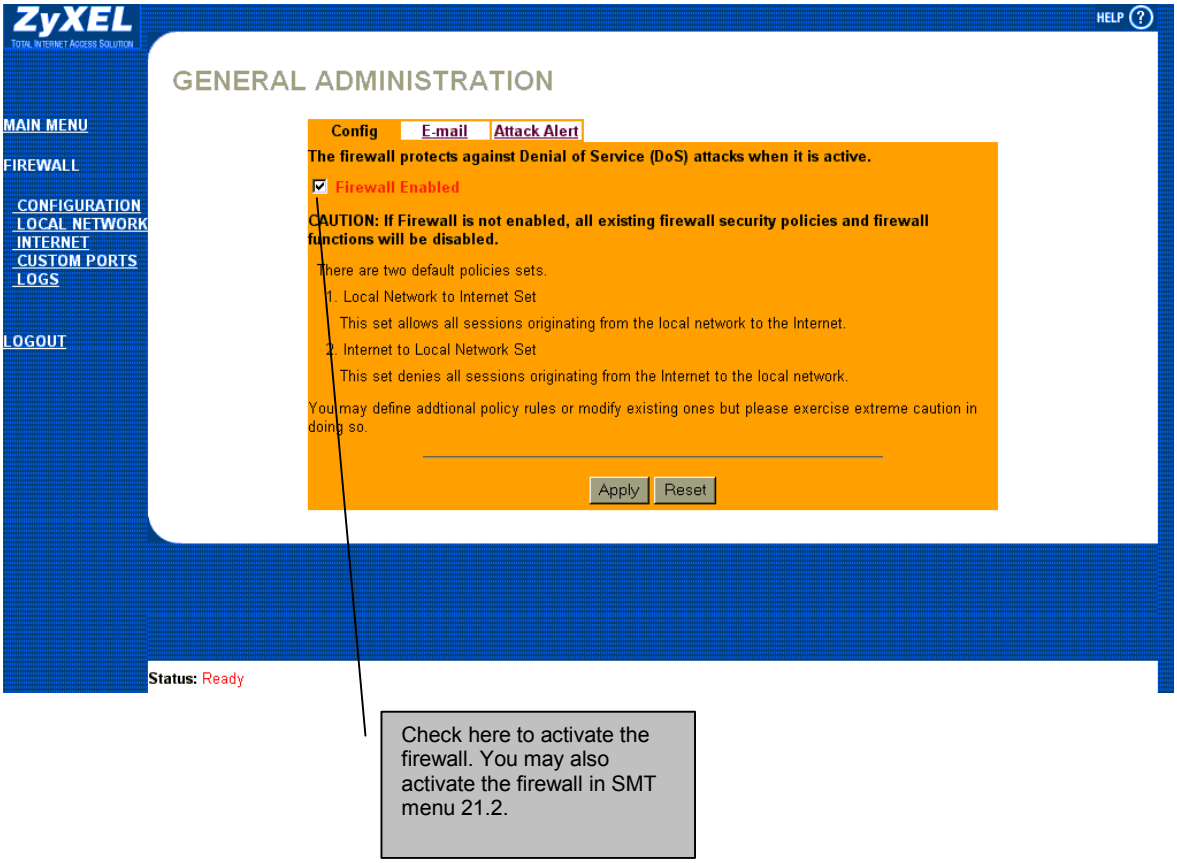
13.1 Examples

Whenever you open a hole in the firewall to forward a service from the Internet to the local network, and NAT is also enabled, you may have to also configure a server behind NAT using SMT menu 15.2. Please see the *NAT chapter*.

13.1.1 Example 1: Firewall Rule To Allow Web Service From The Internet

Let's say you have one server on the local network, with an IP of 10.100.1.2, supporting FTP, HTTP, Telnet and mail services. The only traffic allowed from the Internet is web service. You want to be able to forward all traffic initiated from the local network. You want to know who accesses your server and send e-mail alerts when this happens. Assume, for example, your mail account is user@zyxel.com. Another network administrator has an e-mail address of user2@zyxel.com. Here are the steps you would follow.

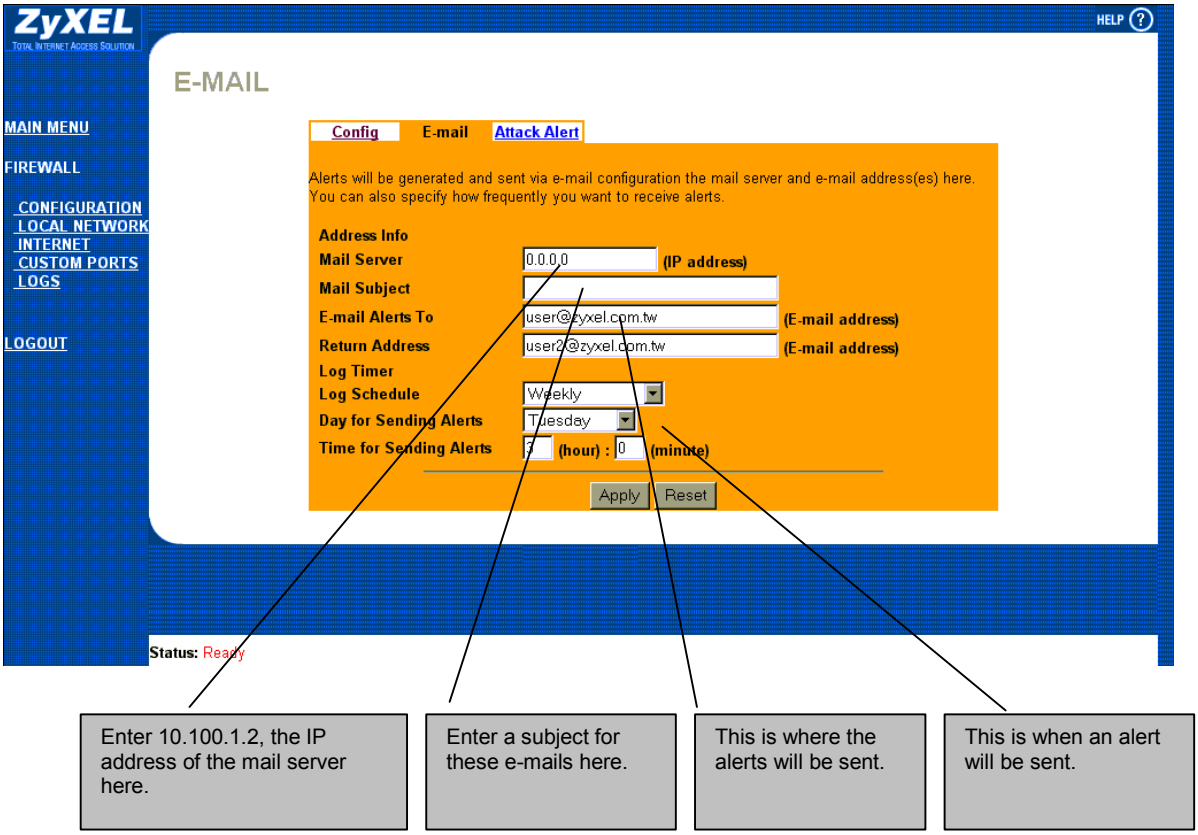
Step 1. Activate the firewall. You may activate the firewall through the web configurator as shown next (click **Configuration**, the **Config** tab, then click the **Firewall Enabled** check box) or through SMT menu 21.2. You can only configure the firewall using the web configurator or CI commands (see *Appendices*). When the firewall is active, the default rules allow all traffic from the local network to the WAN (Internet) and block all traffic from the Internet to the local network.


ZyXEL
TOTAL INTERNET ACCESS SOLUTION
HELP
GENERAL ADMINISTRATION
MAIN MENU
FIREWALL
CONFIGURATION
LOCAL NETWORK
INTERNET
CUSTOM PORTS
LOGS
LOGOUT
Config
E-mail
Attack Alert
The firewall protects against Denial of Service (DoS) attacks when it is active.
Firewall Enabled
CAUTION: If Firewall is not enabled, all existing firewall security policies and firewall functions will be disabled.
There are two default policies sets.
1. Local Network to Internet Set
This set allows all sessions originating from the local network to the Internet.
2. Internet to Local Network Set
This set denies all sessions originating from the Internet to the local network.
You may define addtional policy rules or modify existing ones but please exercise extreme caution in doing so.
Apply
Reset
Status: Ready

Check here to activate the firewall. You may also activate the firewall in SMT menu 21.2.

Figure 13-1 Activate the Firewall

Step 2. Go to the **E-mail** screen by clicking **Advanced**, **Firewall**, **Configuration**, then the **E-mail** tab. Configure the **E-mail** screen as follows.



Enter 10.100.1.2, the IP address of the mail server here.

Enter a subject for these e-mails here.

This is where the alerts will be sent.

This is when an alert will be sent.

Figure 13-2 Example 1: E-Mail Screen

Step 3. Configure your firewall rule as shown in the following screen. The default firewall blocks all Internet traffic entering our local network, but you want to create a hole for web service from the Internet. Click **Internet** and go to the **Rule Summary.** Configure this screen as shown.

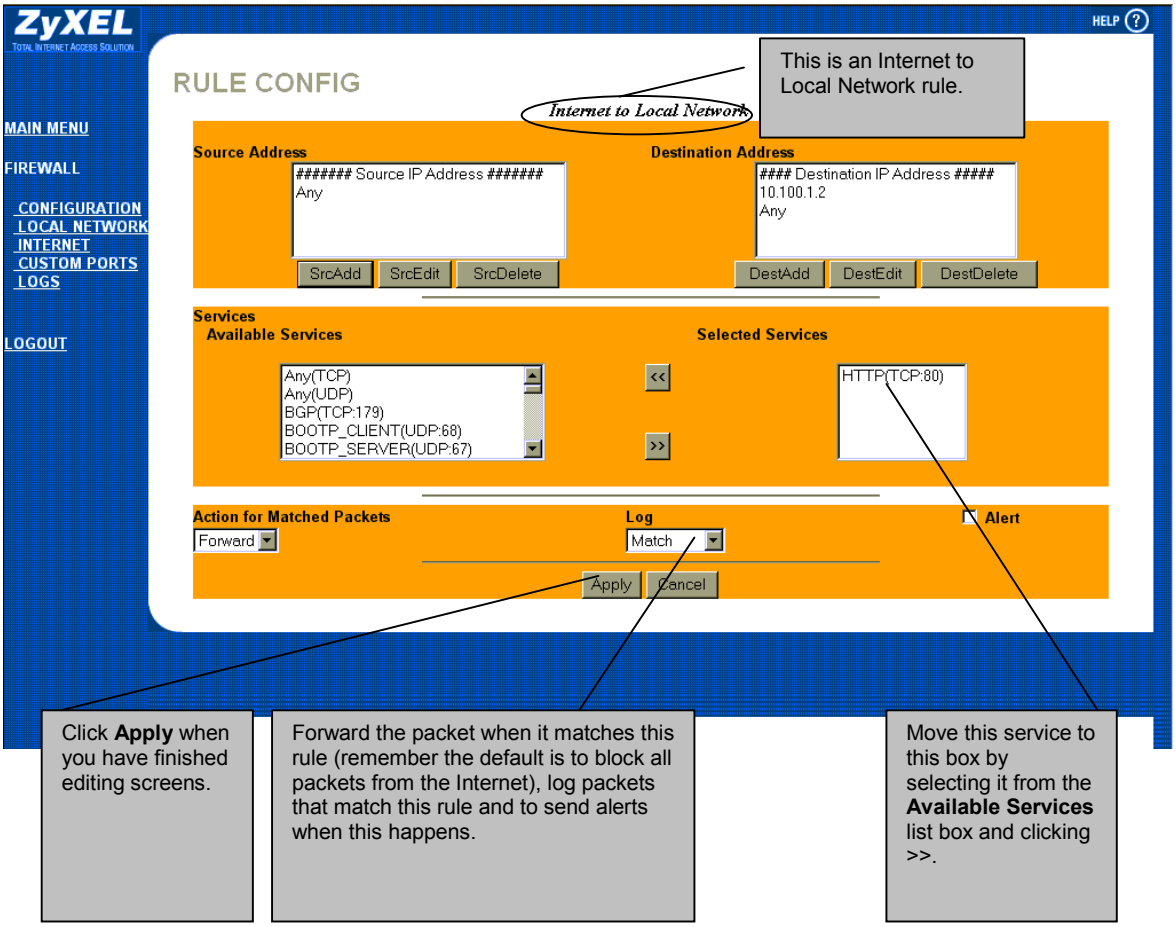


Figure 13-3 Example 1: Configuring a Rule

Step 4. Click **DestAdd** in the previous screen to configure the destination address as the IP of your server on the LAN.

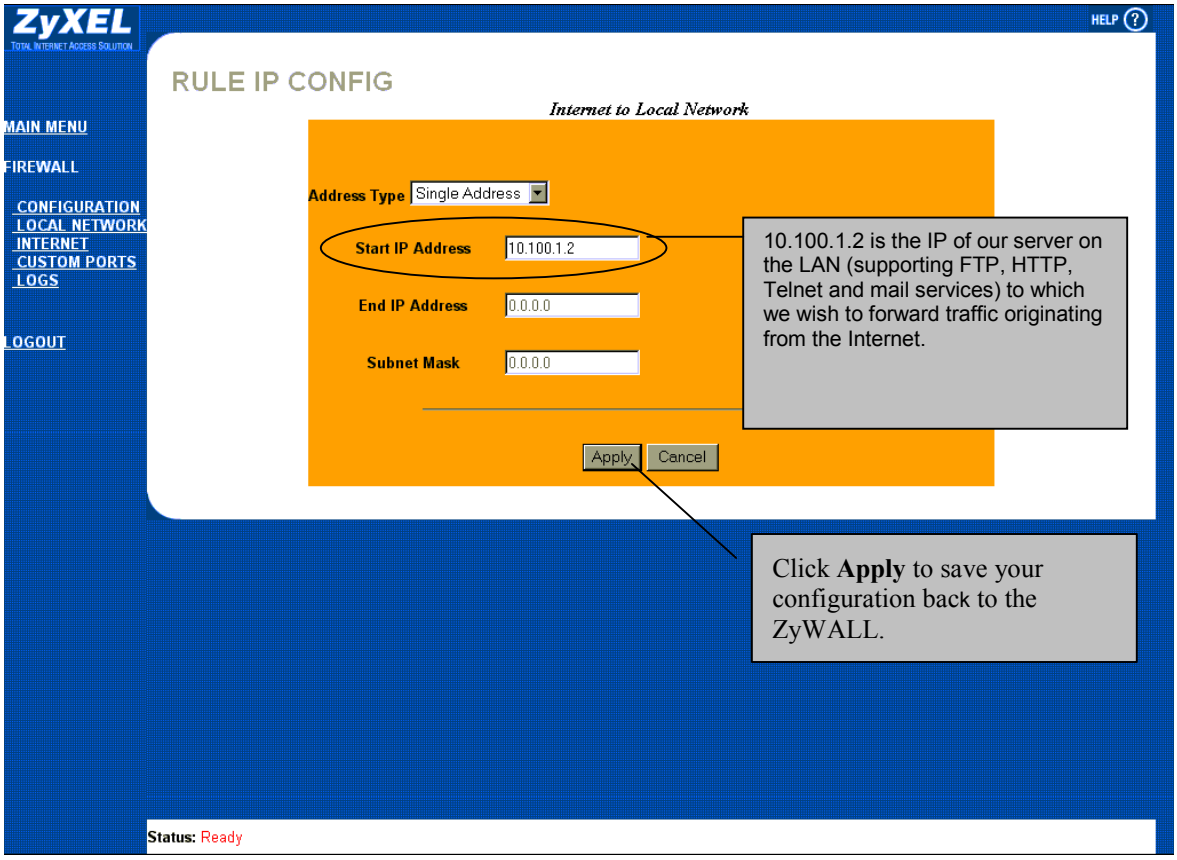


Figure 13-4 Example 1: Destination Address for Traffic Originating from the Internet

Step 5. When you have finished configuring your rules, the Rule Summary screen should look like this. Click **Apply** in this screen to save your configuration back to the ZyWALL.

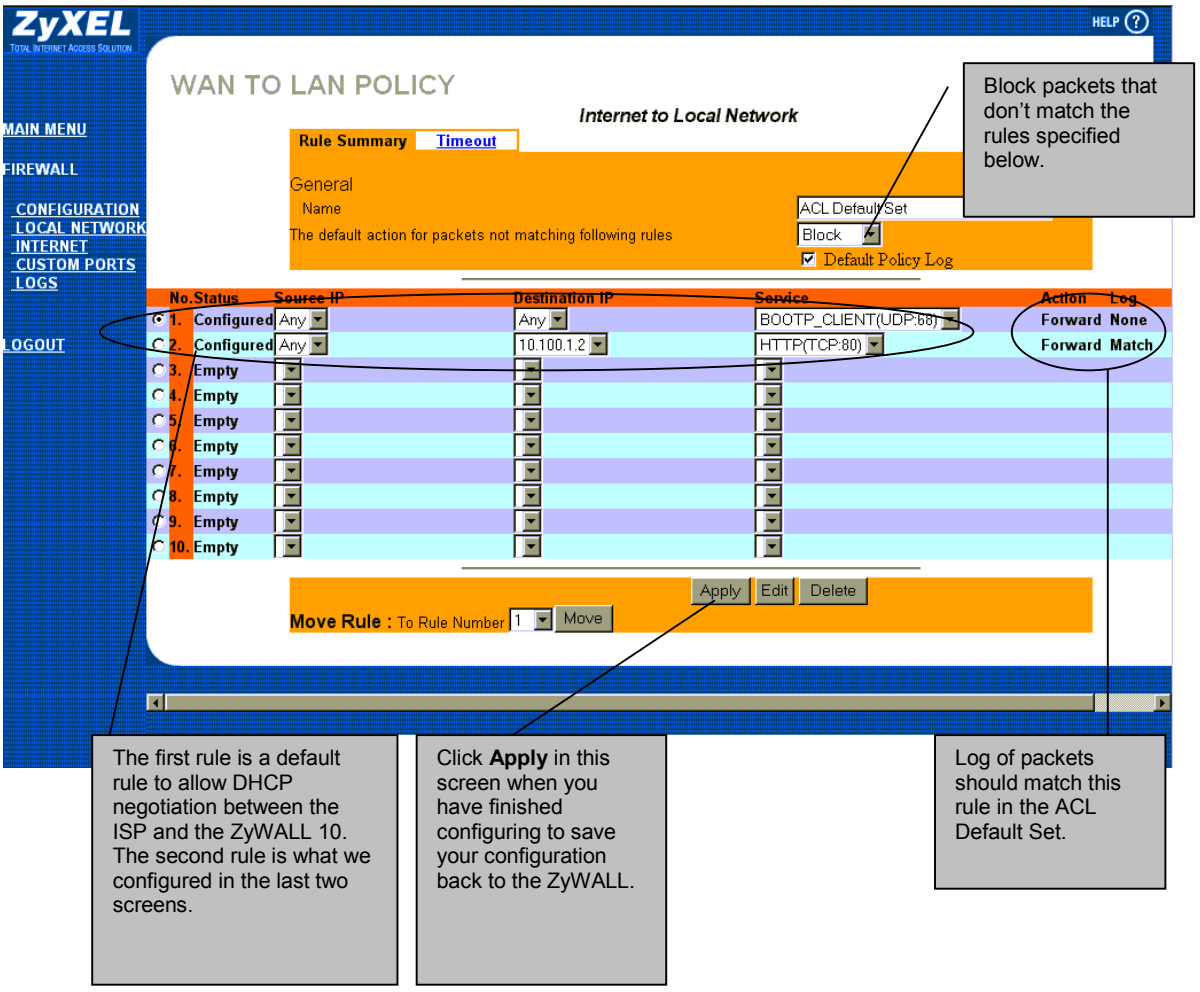

ZyXEL
HELP
WAN TO LAN POLICY
Internet to Local Network
MAIN MENU
FIREWALL
CONFIGURATION
LOCAL NETWORK
INTERNET
CUSTOM PORTS
LOGS
LOGOUT
Rule Summary
Timeout
General
Name
ACL Default Set
The default action for packets not matching following rules
Block
Default Policy Log
No. Status Source IP Destination IP Service Action Log
1. Configured Any Any BOOTP_CLIENT(UDP:68) Forward None
2. Configured Any 10.100.1.2 HTTP(TCP:80) Forward Match
3. Empty
4. Empty
5. Empty
6. Empty
7. Empty
8. Empty
9. Empty
10. Empty
Apply
Edit
Delete
Move Rule : To Rule Number 1 Move
Block packets that don't match the rules specified below.
The first rule is a default rule to allow DHCP negotiation between the ISP and the ZyWALL 10. The second rule is what we configured in the last two screens.
Click Apply in this screen when you have finished configuring to save your configuration back to the ZyWALL.
Log of packets should match this rule in the ACL Default Set.

Figure 13-5 Example 1: Rule Summary Screen

13.1.2 Example 2: Small Office With Mail, FTP and Web Servers

A small office has:

i. A mail server with an IP of 192.168.10.2.

ii. Two FTP servers. You want FTP server 1 (IP of 192.168.10.3) to be accessible from the Internet, but FTP server 2 (192.168.10.4) may only be accessed by internal users, i.e., from the local network.

iii. HTTP proxy server at 192.168.10.5.

You want:

i. To send alerts when there is an attack.

ii. To only allow access to the Internet from the HTTP proxy server and your mail server.

iii. To only allow FTP server 1 to be accessible from the Internet.

Step 1. First you want to send alerts when there is an attack. Go to the **Attack Alert** screen (click **Configuration**, then the **Attack Alert** tab) shown next.

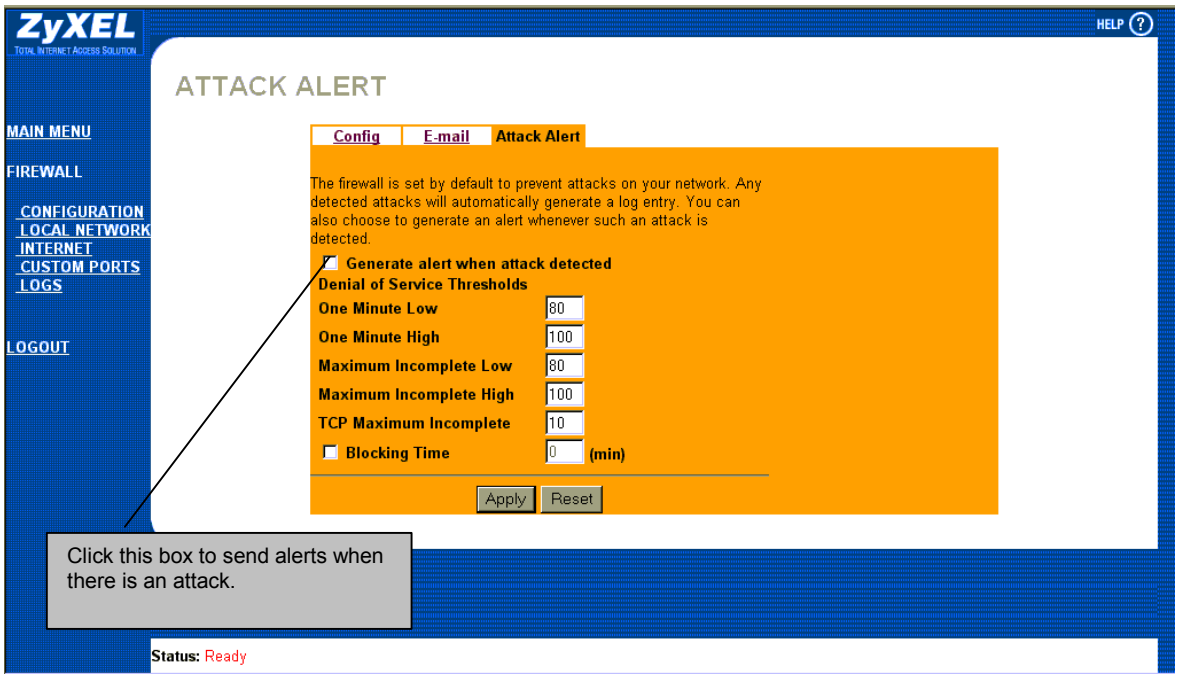


Figure 13-6 Send Alerts When Attacked

Step 2. Configure the **E-mail** screen as shown in example 1: your mail server's IP is 192.168.10.2.

Step 3. Now you want to restrict access to the Internet except for the HTTP proxy server and your mail server. First you need to create a custom port for POP3. POP (Post Office Protocol) is an Internet mail server protocol that provides an incoming message storage system. It works in conjunction with the SMTP (Simple Mail Transfer Protocol), which provides the message transport services required to move mail from one system to another. The current version is called POP3. Click **Custom Ports** and then click **Edit**. Configure the screen as follows.

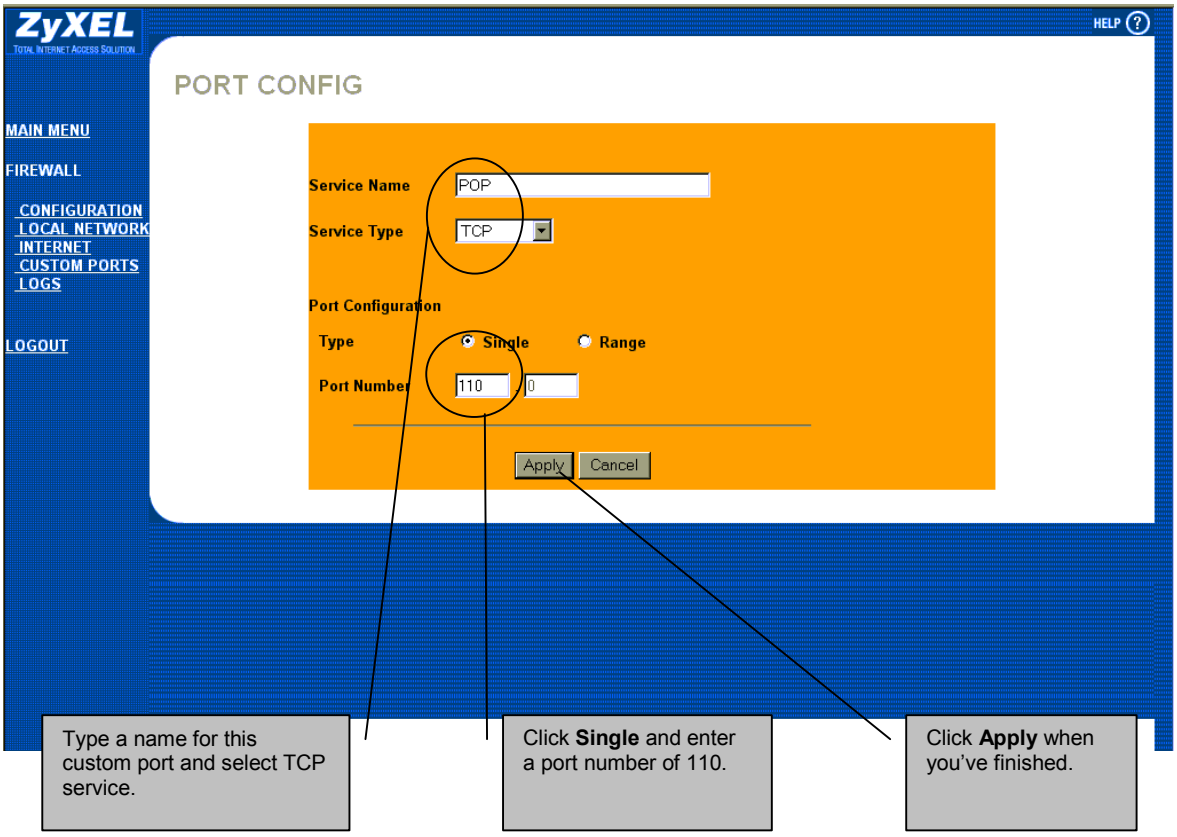


Figure 13-7 Configuring A POP Custom Port

Step 4. Now, you will create rules to block all outgoing traffic (from the local network to the Internet) except for traffic originating from the HTTP proxy server and our mail server. Click **Local**

Network to see the **Rule Summary** screen. Now click an available **No.** (rule number) button, then click **Edit** to bring up the next screen.

Step 5. Click **SrcAdd** under the **Source Address** box and enter the IP address of the mail server (192.168.10.2) in the same fashion as in *Figure 13-4*.

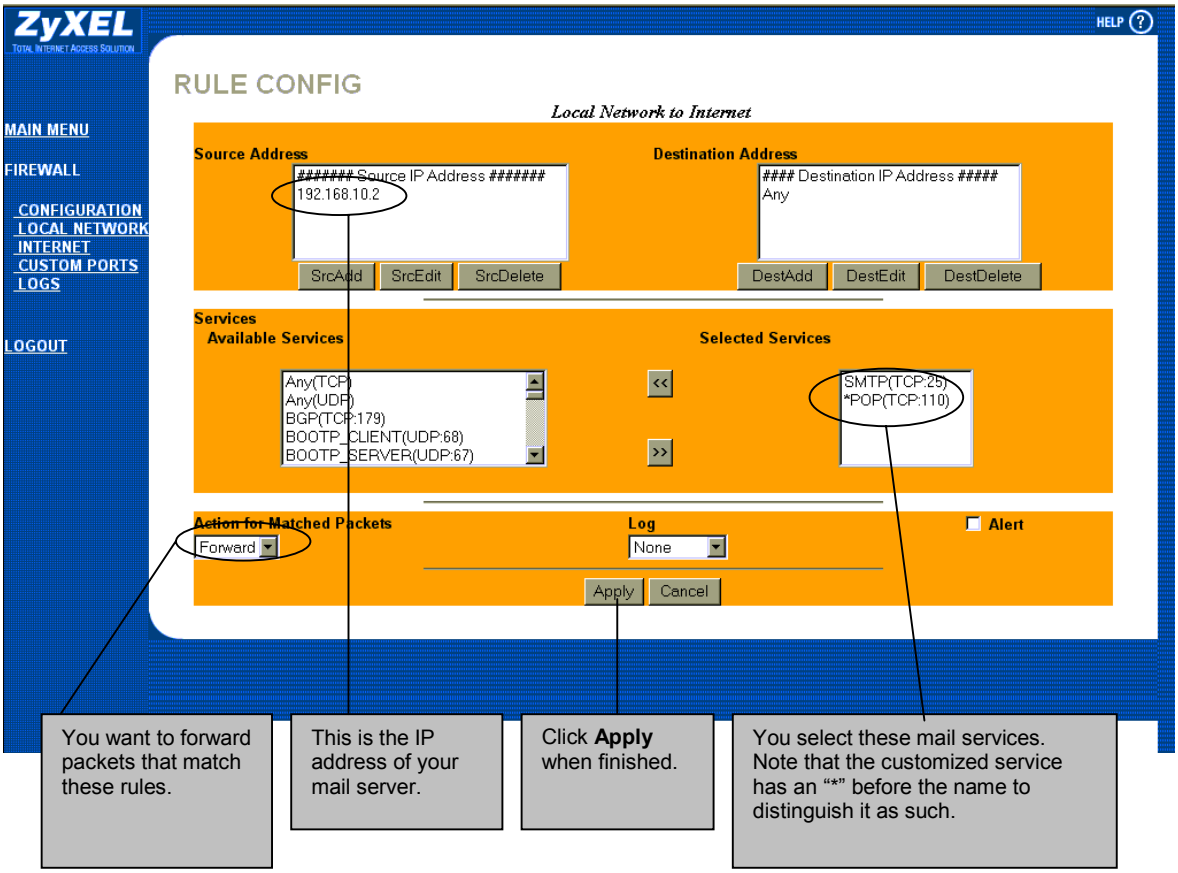


Figure 13-8 Example 2: Local Network Rule 1 Configuration

Step 6. Similarly configure another local network to Internet rule allowing traffic from our web (HTTP) proxy server.

Step 7. The **Rule Summary** screen should look like *Figure 13-9*. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.

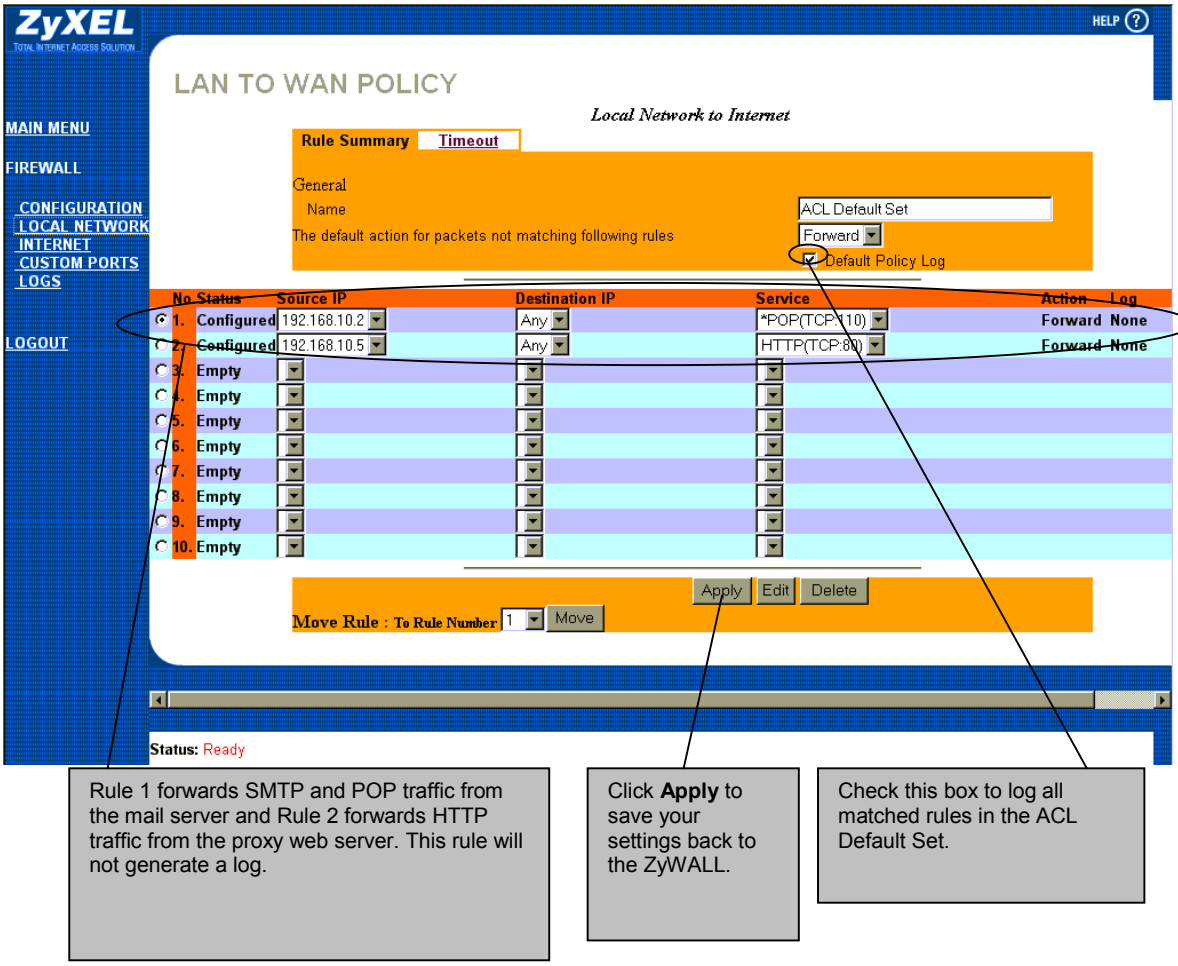


Figure 13-9 Example 2: Local Network Rule Summary

Step 8. Now you want an FTP server (IP of 192.168.10.3) to be accessible from the Internet. Remember the default Internet to Local Network ACL Set blocks all traffic from the Internet, so you want to create a hole for this server. Click the **Internet** link to see its **Rule Summary** screen. Now click an available **No.** (rule number) radio button, then click **Edit** to bring up the **Rule Config**(uration)

screen. Now click on the **DestAdd** button under the **Destination Address** box and enter the IP of FTP server One (192.168.10.3).

Step 9. On completing the procedure the **Rule Summary** for this Internet firewall rule should look like the following screen. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.

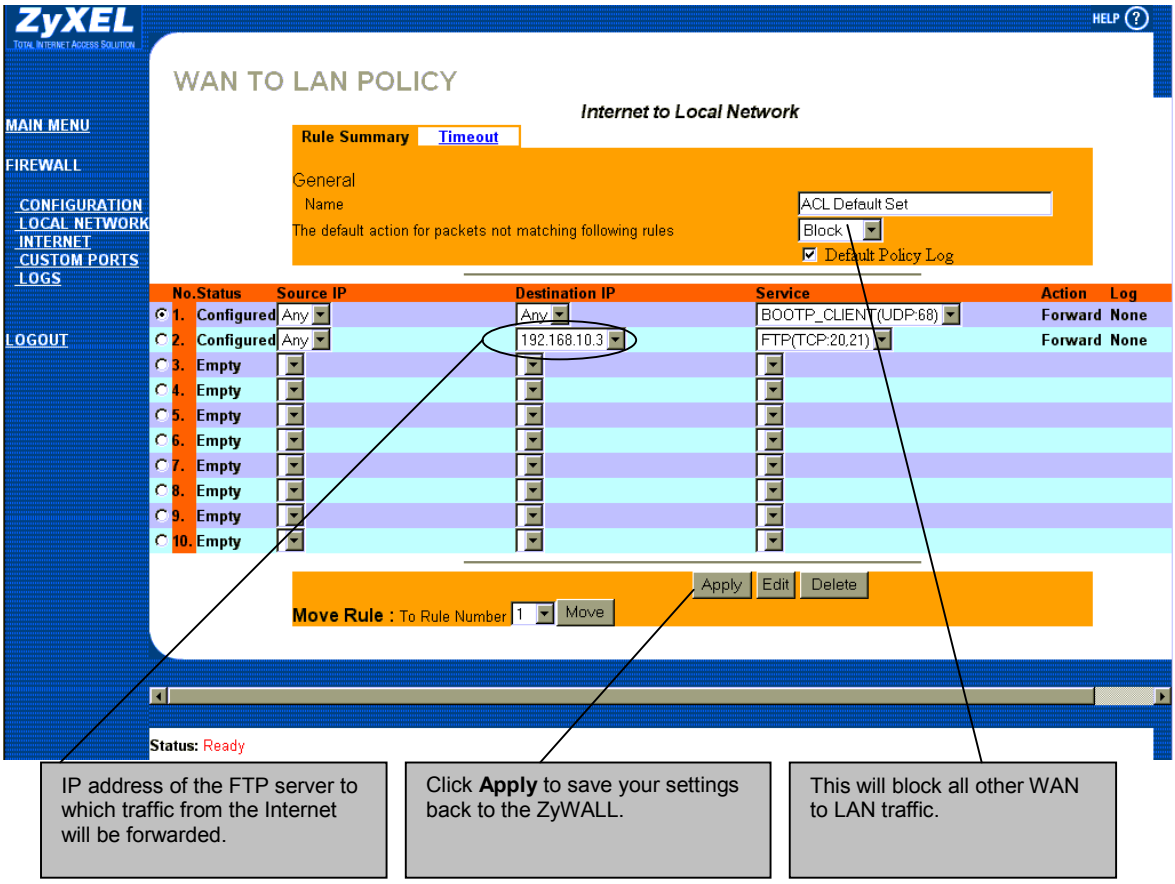


Figure 13-10 Example: Internet to Local Network Rule Summary

13.1.3 Example 3: DHCP Negotiation and Syslog Connection from the Internet

The following are some Internet firewall rule examples that allow DHCP negotiation between the ISP and the ZyWALL and allow a syslog connection from the Internet. Follow the procedure shown next to first configure a custom port.

Step 1. Click the **Custom Ports** link and then click **Edit** to display the following screen.

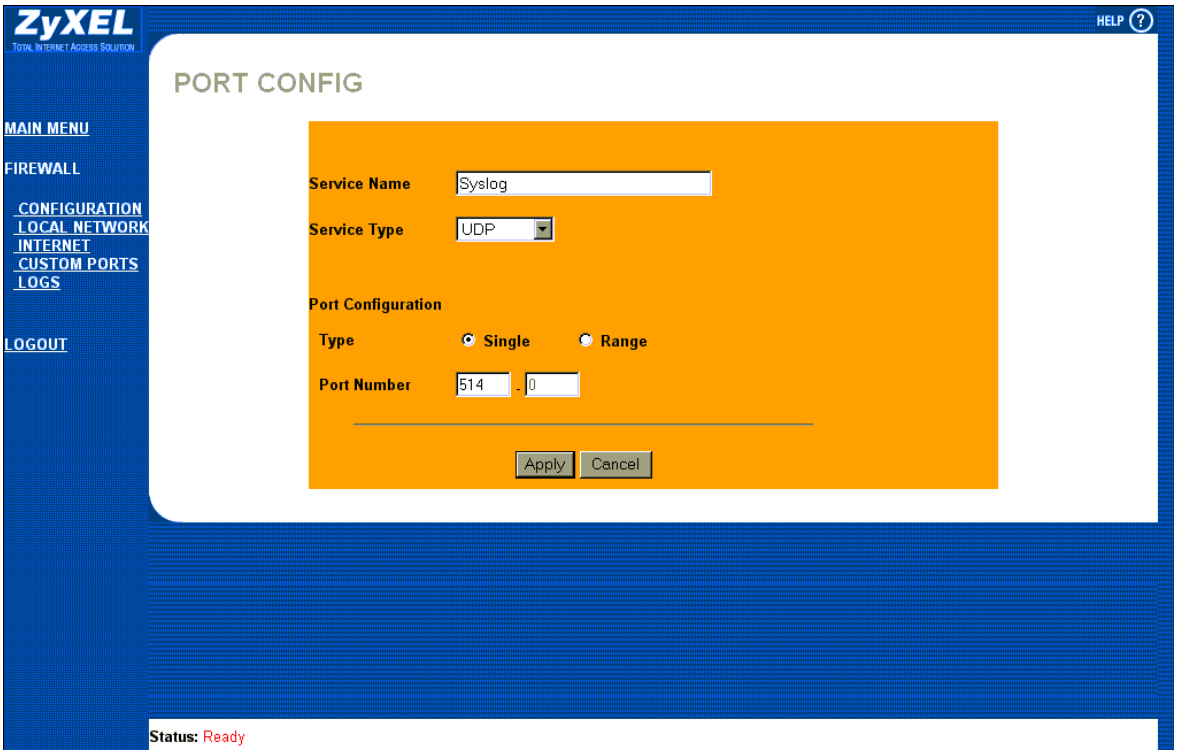


Figure 13-11 Custom Port for Syslog

Custom ports show up with an "*" before their names in the Services **list box and the Rule Summary list box. Click** Apply **after you've created your custom port.**

Step 2. Follow the procedures outlined in the previous examples to configure all your rules. You should configure the rule configuration screen like the one below and apply it.

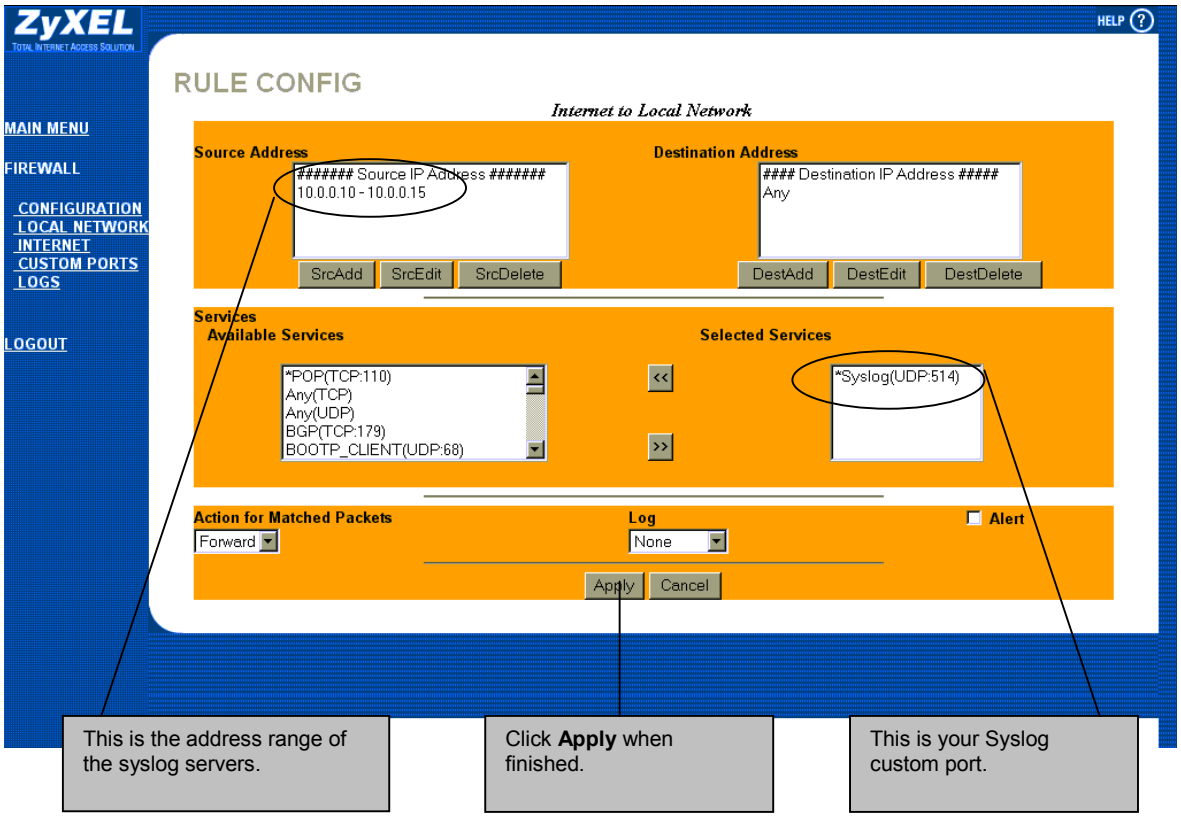


Figure 13-12 Syslog Rule Configuration

Step 3. On completing the configuration procedure for these Internet firewall rules, the **Rule Summary** screen should look like the following. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.

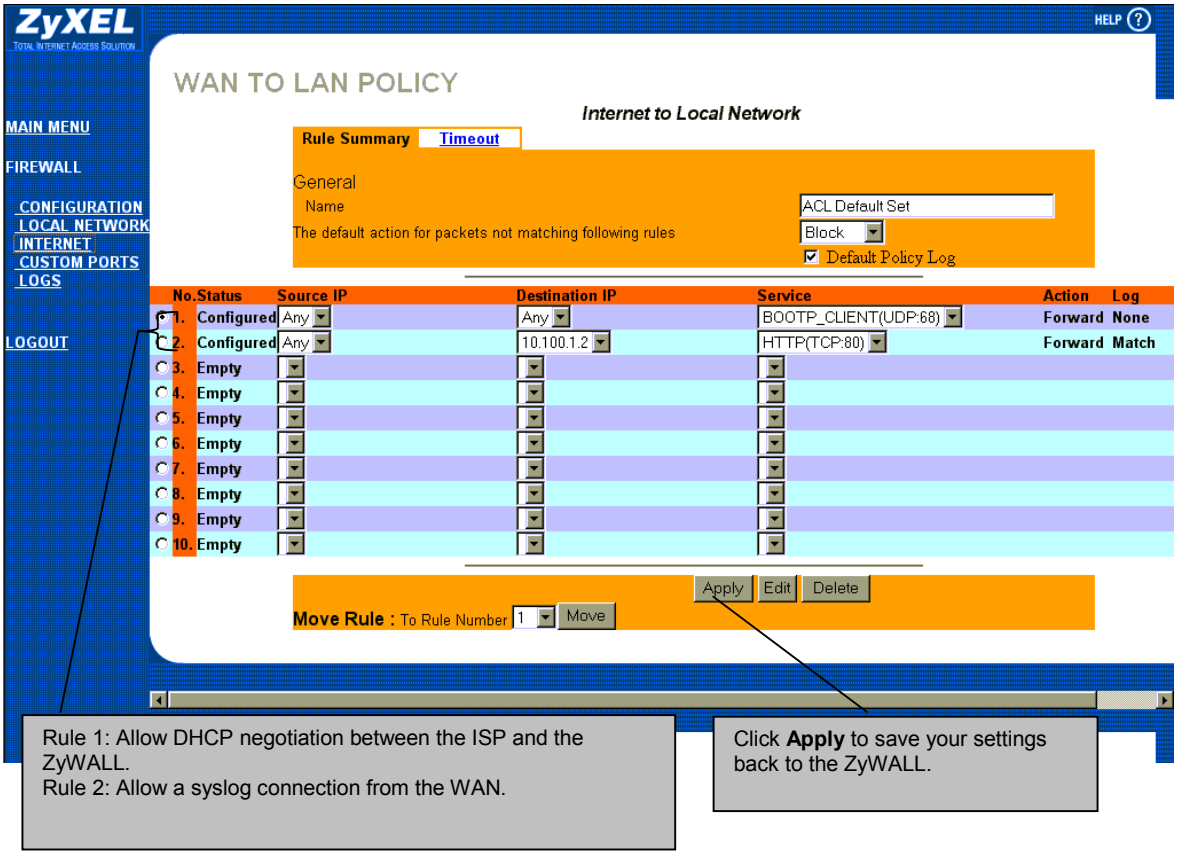


Figure 13-13 Example 3: Rule Summary

Chapter 14
Content Filtering

This chapter provides a brief overview of content filtering using the web embedded configurator. For more detailed information, consult the embedded HTML help.

Internet content filtering allows schools and businesses to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URLs and should not be confused with packet filtering via SMT menu 21.1. To access these functions, from the **Main Menu**, click **Advanced**, then **Content Filter** to expand the Content Filter menus.

14.1 Categories

14.1.1 Restrict Web Features

The ZyWALL can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

14.1.2 Filter List

The administrator can select categories, such as pornography or racial intolerance, to block or monitor from a pre-defined list. There is a period of free use of the list when you register the ZyWALL. After this period, you must subscribe to the list periodically.

14.1.3 Days and Times

The ZyWALL also allows the administrator to define time periods and days during which content filtering should be enabled.

14.2 Update List

Content on the Internet is constantly changing, so the content filter list should be updated on a weekly basis.

14.3 Exempt Computers

This link allows the administrator to include or exclude a range of users on the LAN from content filtering.

14.4 Customizing

Customize the content filter list by adding or removing specific sites from the filter list.

14.5 Keywords

The ZyWALL can also be configured to block certain Web sites by using URL keywords.

14.6 Log Records

This screen records the results of your content filter policies

Part IV:

Advanced Management

This part provides information on Filter Configuration, SNMP Configuration, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Information and Remote Management.

Chapter 15
Filter Configuration

This chapter shows you how to create and apply filters.

15.1 About Filtering

Your ZyWALL uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

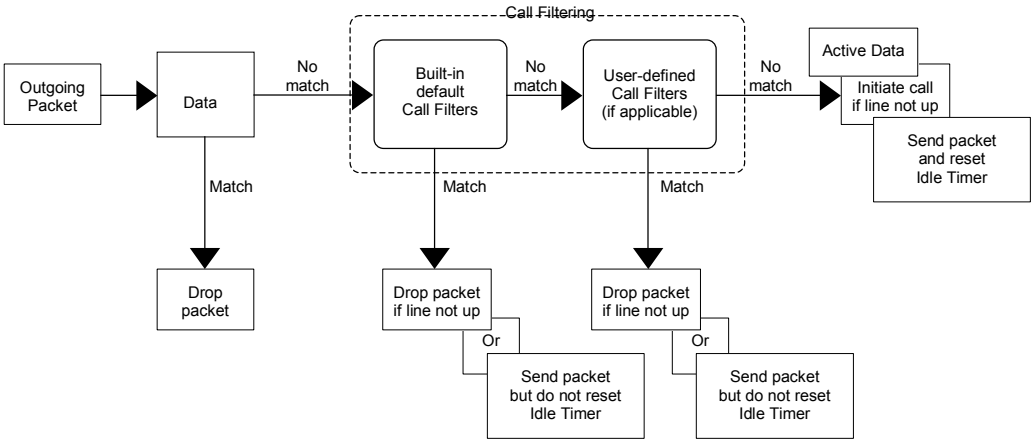


Figure 15-1 Outgoing Packet Filtering Process

For incoming packets, your ZyWALL applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

15.1.1 The Filter Structure of the ZyWALL

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyWALL allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnetting. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also *Figure 15-9* for the logic flow when executing an IP filter.

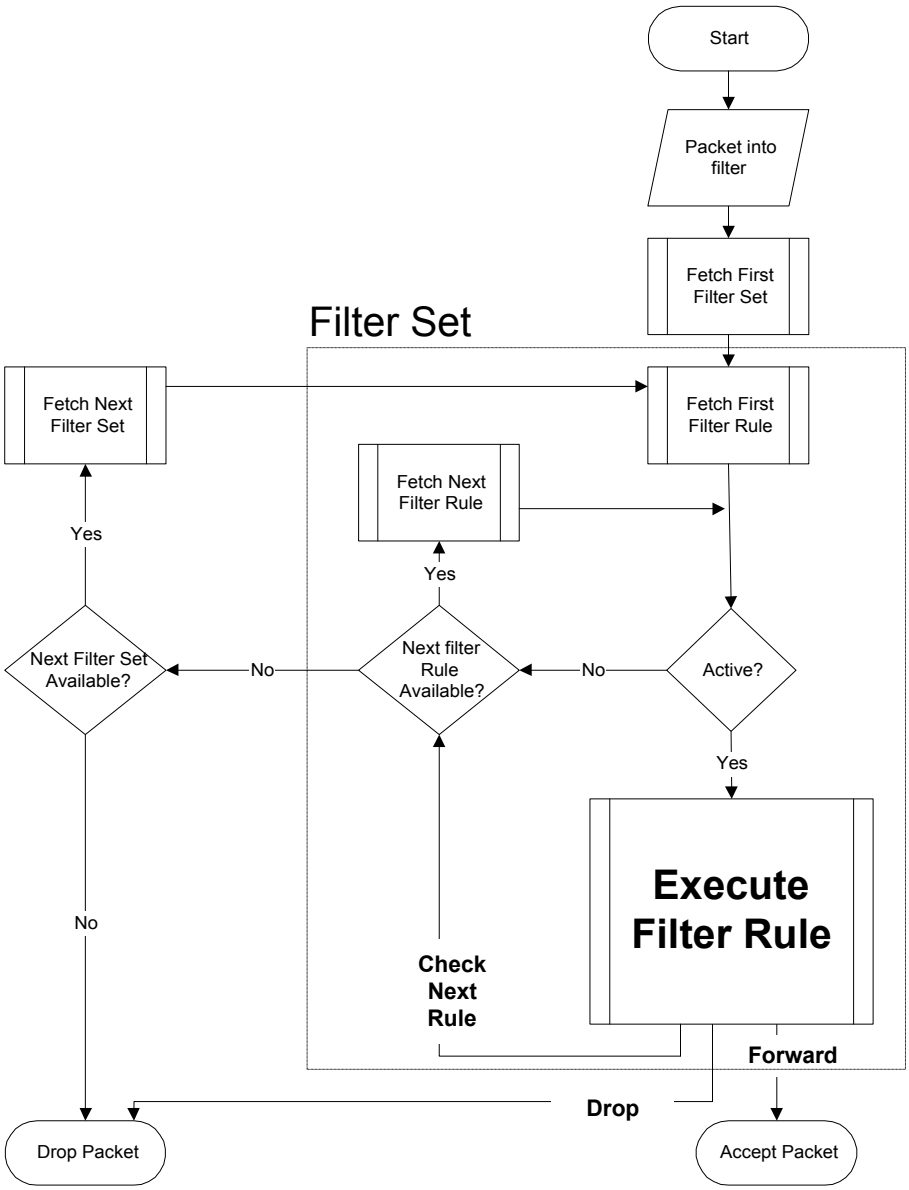


Figure 15-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

15.2 Configuring a Filter Set

To configure a filter set, follow the procedure below. For more information on menus 21.2 and 21.3, please see the firewall chapters.

Step 1. Select option 21. **Filter Set Configuration** from the main menu to open menu 21.

```
                Menu 21 - Filter and Firewall Setup

                        1. Filter Setup
                        2. Firewall Setup
                        3. View Firewall Log




                              Enter Menu Selection Number:
```

Figure 15-4 Menu 21 — Filter and Firewall Setup

Step 2. Enter 1 to bring up the following menu.

```
                Menu 21.1 - Filter Set Configuration

Filter                                  Filter
Set #        Comments                   Set #        Comments
------  -----------------               ------  -----------------
  1      NetBIOS_WAN                      7      _________________
  2      NetBIOS_LAN                      8      _________________
  3      _________________                9      _________________
  4      _________________               10      _________________
  5      _________________               11      _________________
  6      _________________               12      _________________

                Enter Filter Set Number to Configure= 0

                Edit Comments= N/A

                Press ENTER to Confirm or ESC to Cancel:
```

Figure 15-5 Menu 21.1 — Filter Set Configuration

Step 3. Select the filter set you wish to configure (1-12) and press [ENTER].

Step 4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

```
                    Menu 21.1.1 - Filter Rules Summary

 # A Type                        Filter Rules                       M m n
 - - ---- ------------------------------------------- --------- - - -
   1 Y IP   Pr=6,  SA=0.0.0.0, DA=0.0.0.0, DP=137                   N D N
   2 Y IP   Pr=6,  SA=0.0.0.0, DA=0.0.0.0, DP=138                   N D N
   3 Y IP   Pr=6,  SA=0.0.0.0, DA=0.0.0.0, DP=139                   N D N
   4 Y IP   Pr=17,  SA=0.0.0.0, DA=0.0.0.0, DP=137                  N D N
   5 Y IP   Pr=17,  SA=0.0.0.0, DA=0.0.0.0, DP=138                  N D N
   6 Y IP   Pr=17,  SA=0.0.0.0, DA=0.0.0.0, DP=139                  N D F


                  Enter Filter Rule Number (1-6) to Configure:



                    Press ENTER to Confirm or ESC to Cancel:
```

Figure 15-6 NetBIOS_WAN Filter Rules Summary

```
                    Menu 21.1.2 - Filter Rules Summary

# A Type                        Filter Rules                       M m n
 - - ---- ------------------------------------------- --------- - - -
  1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53           N D F
  2 Y
  3 Y
  4 Y
  5 Y
  6 Y

  Enter Filter Rule Number (1-6) to Configure:
```

Figure 15-7 NetBIOS _LAN Filter Rules Summary

15.2.1 Filter Rules Summary Menu

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 15-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 15-2 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address

Table 15-2 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

15.2.2 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyWALL will warn you and will not allow you to save.

15.2.3 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, e.g., UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1 - TCP/IP Filter Rule**, as shown next.

```
                    Menu 21.1.1.1 - TCP/IP Filter Rule

          Filter #: 1,1
          Filter Type= TCP/IP Filter Rule
          Active= Yes
          IP Protocol= 6      IP Source Route= No
          Destination: IP Addr= 0.0.0.0
          IP Mask= 0.0.0.0
          Port #= 137
          Port # Comp= Equal
          Source: IP Addr= 0.0.0.0
          IP Mask= 0.0.0.0
          Port #=
          Port # Comp= None
          TCP Estab= No
          More= No              Log= None
          Action Matched= Drop

          Action Not Matched= Check Next Rule

          Press ENTER to Confirm or ESC to Cancel:
          Press Space Bar to Toggle.
```

Figure 15-8 Menu 21.1.1.1 — TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 15-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Active	**Yes** activates the filter rule and **No** deactivates it.	**Yes**/**No**
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	If **Yes**, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	**Yes**/**No**
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.	0.0.0.0

Table 15-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**.	**None/Less/Greater/Equal/Not Equal]**
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.	**None/Less/Greater/Equal/Not Equal**
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.	**Yes/No**
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**Yes/No**
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet. .	**Check Next Rule** **Forward**

Table 15-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
		Drop
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
Press [SPACE BAR] to select properties for fields that do not need to be typed in. When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.		

The following figure illustrates the logic flow of an IP filter.

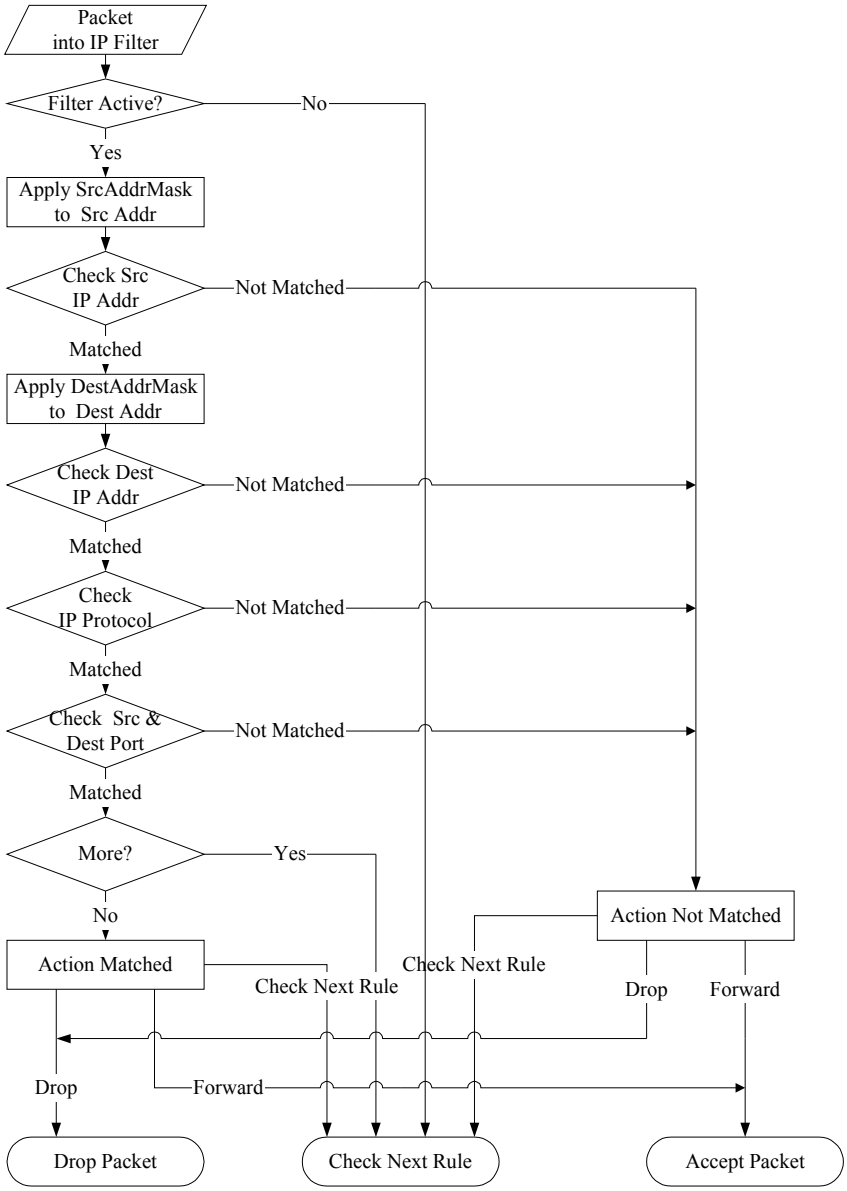


Figure 15-9 Executing an IP Filter

15.2.4 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyWALL treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyWALL applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, e.g., FFFFFFFF.

To configure a generic rule, select Generic Filter Rule in the Filter Type field in menu 21.4.1.1 and press [ENTER] to open Generic Filter Rule, as shown below.

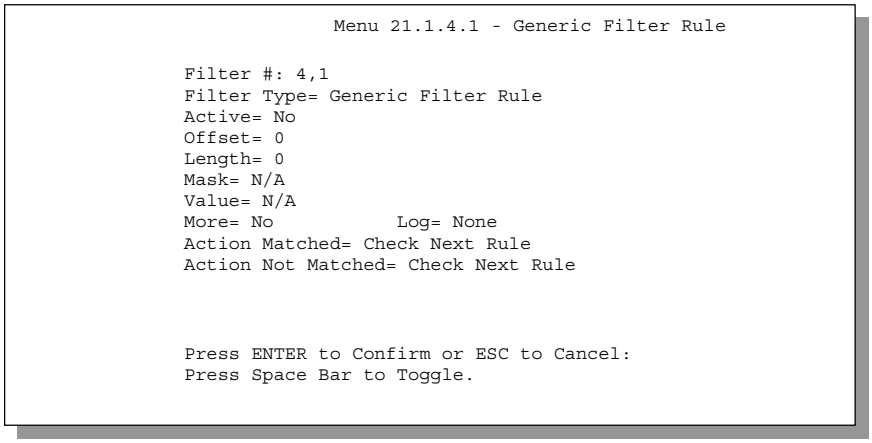

Menu 21.1.4.1 - Generic Filter Rule
Filter #: 4,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

Figure 15-10 Menu 21.4.1.1 — Generic Filter Rule

The following table describes the fields in the Generic Filter Rule Menu.

Table 15-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	**Generic Filter Rule**/ **TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule or **No** to turn it off.	**Yes**
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0 (Default)
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0 (Default)
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**.	**Yes**/**No**
Log	Select the logging option from the following: **None** - No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	 **None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a packet matching the rule.	**Check Next Rule, Forward, Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule, Forward, Drop**

Table 15-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
		Drop
Once you have completed filling in **Menu 21.4.1.1 - Generic Filter Rule**, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.		

15.3 Example Filter

Let's look at an example to block outside users from telnetting into the ZyWALL. Please see our included disk for more example filters.

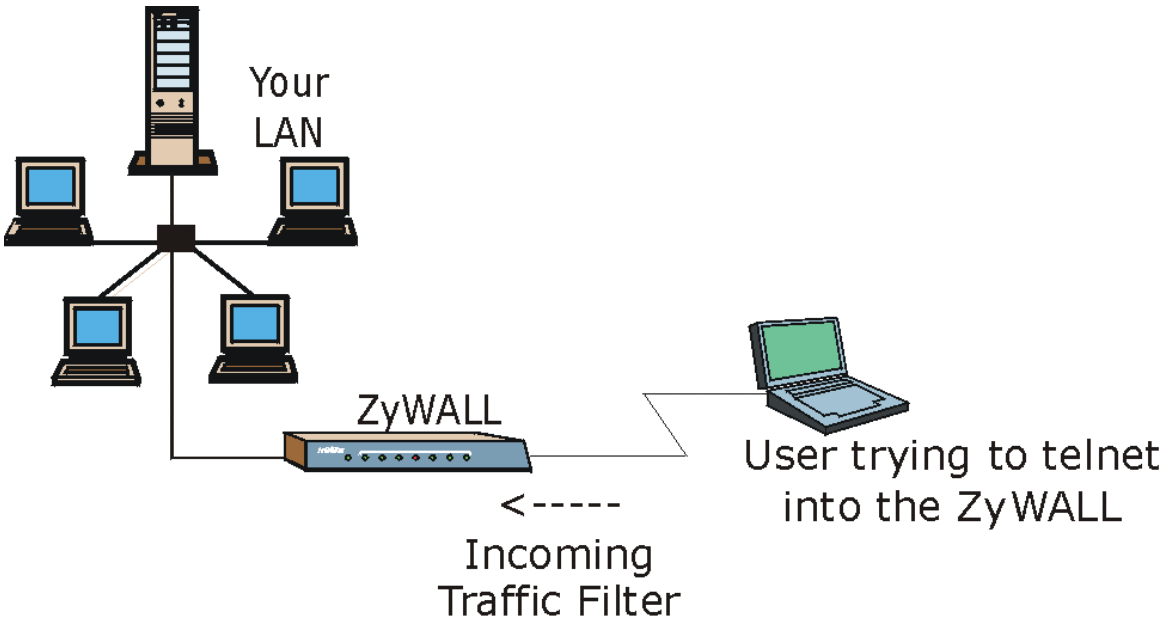


Figure 15-11 Telnet Filter Example

Step 1. Enter 21 from the main menu to open **Menu 21.1 - Filter Set Configuration**.

Step 2. Enter the index of the filter set you wish to configure (say 3) and press [ENTER].

Step 3. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

Step 5. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

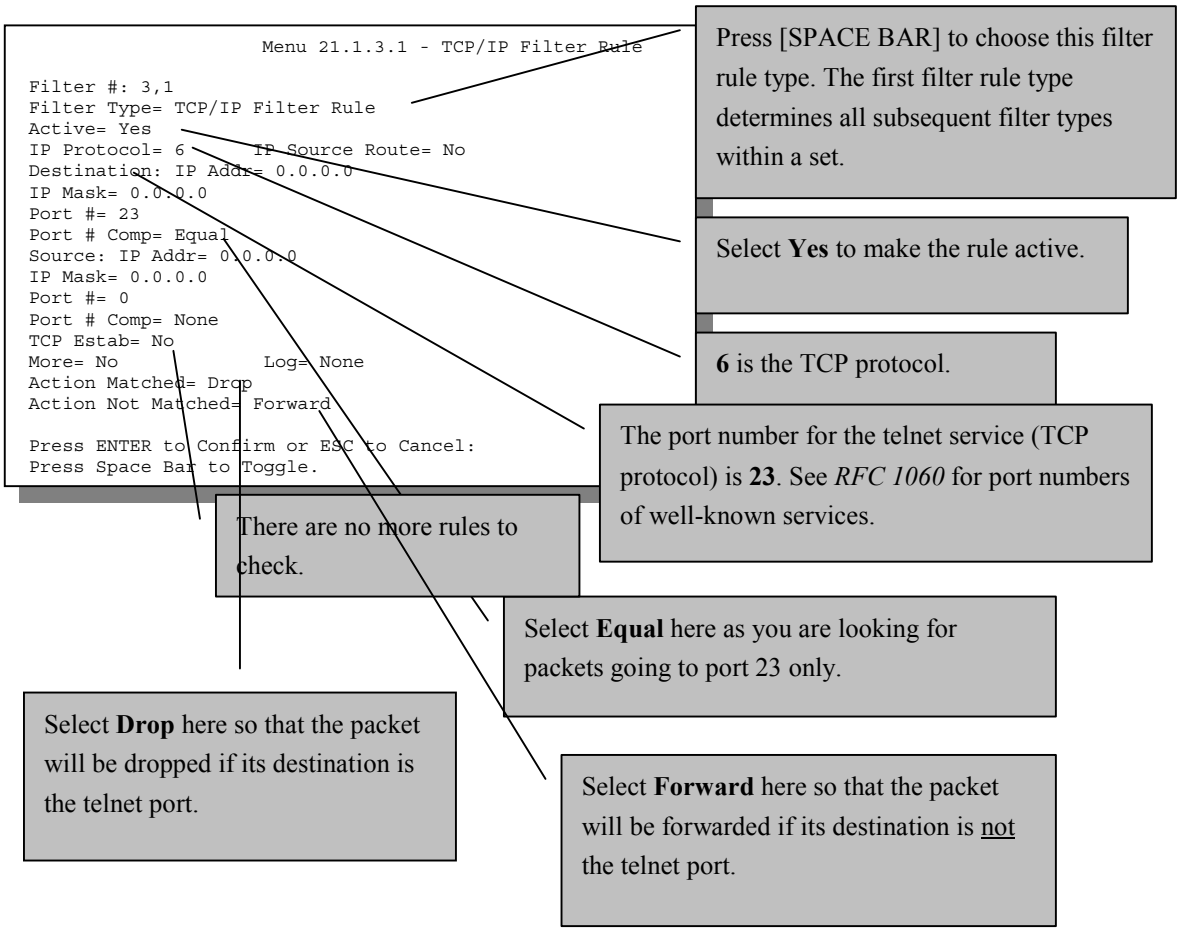

Menu 21.1.3.1 - TCP/IP Filter Rule
Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6 IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 23
Port # Comp= Equal
Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 0
Port # Comp= None
TCP Estab= No
More= No Log= None
Action Matched= Drop
Action Not Matched= Forward
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
Press [SPACE BAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.
Select Yes to make the rule active.
6 is the TCP protocol.
The port number for the telnet service (TCP protocol) is 23. See RFC 1060 for port numbers of well-known services.
There are no more rules to check.
Select Equal here as you are looking for packets going to port 23 only.
Select Drop here so that the packet will be dropped if its destination is the telnet port.
Select Forward here so that the packet will be forwarded if its destination is not the telnet port.

Figure 15-12 Example Filter — Menu 21.1.3.1

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

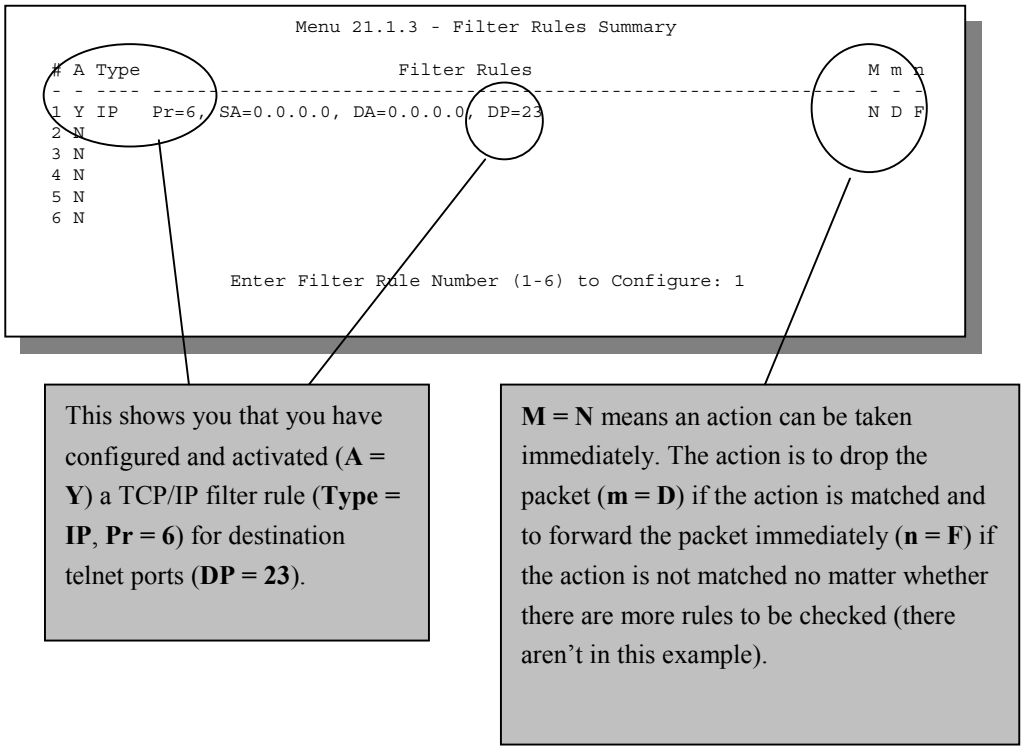

Menu 21.1.3 - Filter Rules Summary
A Type Filter Rules M m n
1 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23 N D F
2 N
3 N
4 N
5 N
6 N
Enter Filter Rule Number (1-6) to Configure: 1
This shows you that you have configured and activated (A = Y) a TCP/IP filter rule (Type = IP, Pr = 6) for destination telnet ports (DP = 23).
M = N means an action can be taken immediately. The action is to drop the packet (m = D) if the action is matched and to forward the packet immediately (n = F) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 15-13 Example Filter Rules Summary — Menu 21.1.3

After you've created the filter set, you must apply it.

Step 1. Enter 11 from the main menu to go to menu 11.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure* 15-16.

Step 4. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

15.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyWALL applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyWALL is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

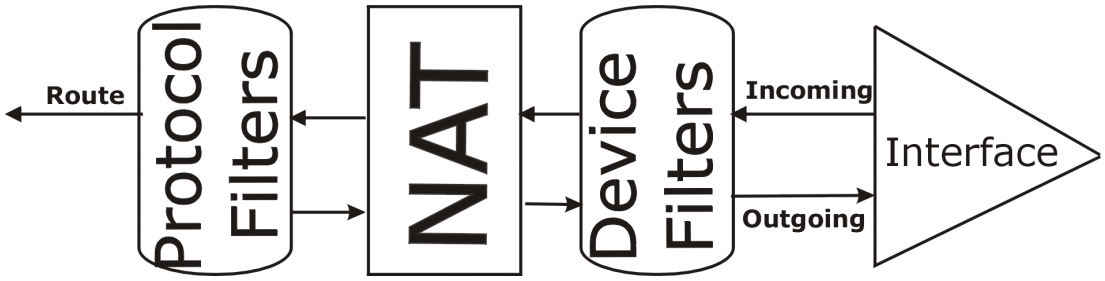


Figure 15-14 Protocol and Device Filter Sets

15.5 Firewall

Firewall configuration is discussed in the firewall chapters of this manual. Further comparisons are also made there between filtering, NAT and the firewall.

15.6 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

If you do not activate the firewall, it is advisable to apply these default filters as shown next.

15.6.1 LAN traffic

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The factory default set, NetBIOS_LAN, can be inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 to block NetBIOS traffic to the ZyWALL from the LAN.

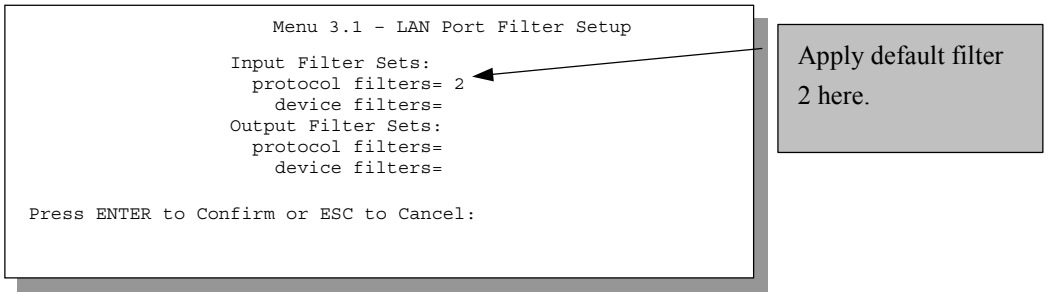


Figure 15-15 Filtering LAN Traffic

15.6.2 Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their

numbers separated by commas. The factory default filter set, NetBIOS_WAN, can be applied in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP (when you are using PPPoE or PPTP encapsulation only). Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation, and in the **protocol filters** field under **Call Filter Sets** when using PPPoE or PPTP encapsulation. Apply them as shown in the following figure.

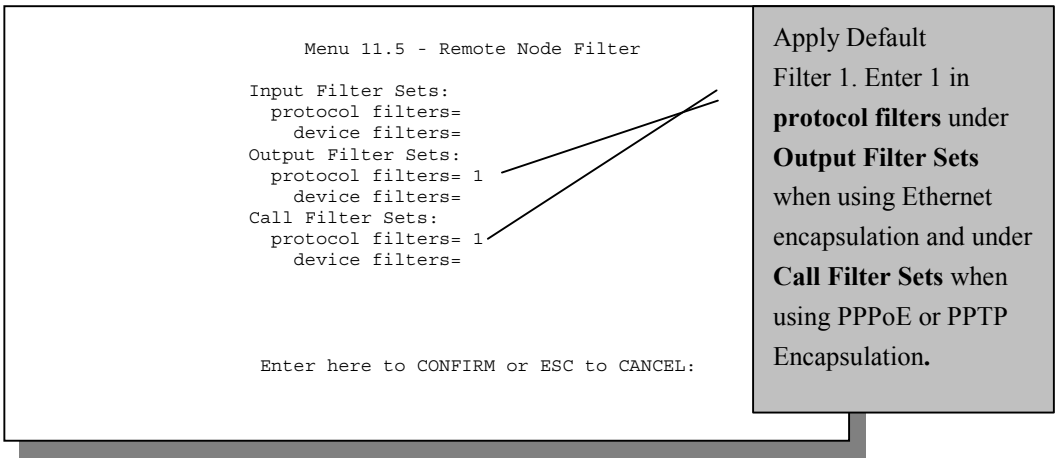

Menu 11.5 - Remote Node Filter
Input Filter Sets:
protocol filters=
device filters=
Output Filter Sets:
protocol filters= 1
device filters=
Call Filter Sets:
protocol filters= 1
device filters=
Enter here to CONFIRM or ESC to CANCEL:
Apply Default Filter 1. Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation and under **Call Filter Sets** when using PPPoE or PPTP Encapsulation.

Figure 15-16 Filtering Remote Node Traffic

Chapter 16
SNMP Configuration

This chapter discusses SNMP for network management and monitoring.

16.1 About SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation.

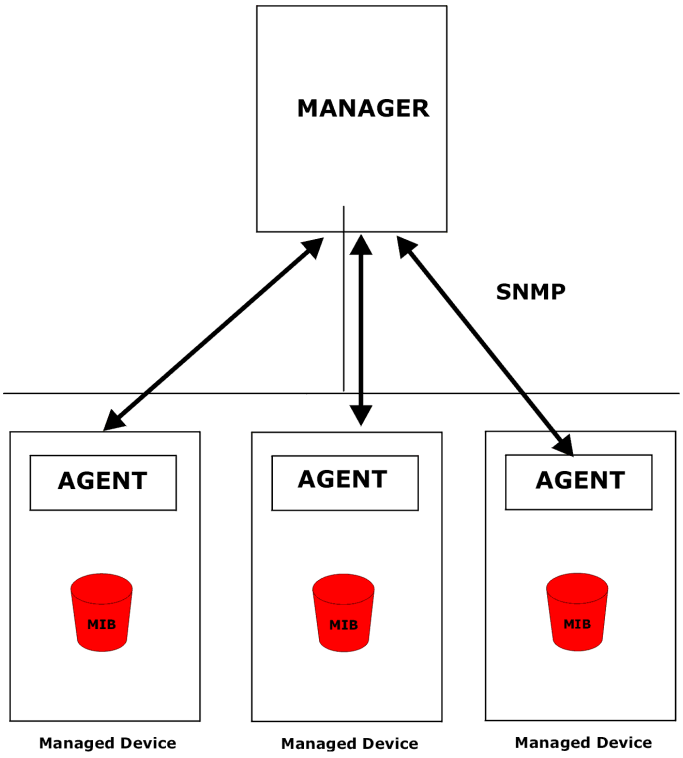


Figure 16-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model

Table 16-1 General SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

16.2 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The ZyWALL can also respond with specific data from the ZyXEL private MIB (ZYXEL-MIB). The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

The ZyWALL acts as an SNMP agent. Users must implement their own GUI on SNMP platform (SNMP manager).

16.3 Configuring SNMP

To configure SNMP, select **SNMP Configuration** (enter 22) from the main menu to open **Menu 22 - SNMP Configuration**, as shown in the figure below. The "community" for Get, Set and Trap fields is simply SNMP's terminology for password.

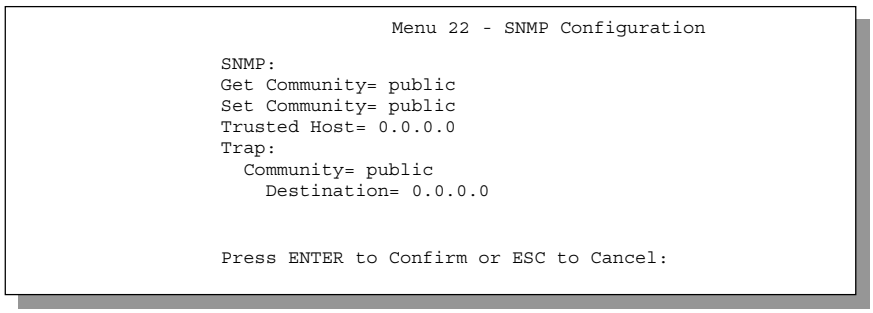


Figure 16-2 Menu 22 — SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 16-2 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	DEFAULT
Get Community	Enter the **Get Community**, which is the password for the incoming Get- and GetNext- requests from the management station.	public (default)
Set Community	Enter the **Set Community**, which is the password for incoming Set- requests from the management station.	public (default)
Trusted Host	If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. If you leave the field set to 0.0.0.0 (default), your ZyWALL will respond to all SNMP messages it receives, regardless of source.	0.0.0.0 (default)
Trap: Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.	public (default)
Trap: Destination	Enter the IP address of the station to send your SNMP traps to.	0.0.0.0 (default)
Once you have completed filling in **Menu 22 - SNMP Configuration**, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel.		

16.4 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

Table 16-3 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warmstart).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (e.g. download new files, CI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

Chapter 17
System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4.

This chapter covers the diagnostic tools that help you to maintain your ZyWALL. These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.

```
                    Menu 24 - System Maintenance

                        1.  System Status
                        2.  System Information and Console Port Speed
                        3.  Log and Trace
                        4.  Diagnostic
                        5.  Backup Configuration
                        6.  Restore Configuration
                        7.  Upload Firmware
                        8.  Command Interpreter Mode
                        9.  Call Control
                        10. Time and Date Setting
                        11. Remote Management Setup



                         Enter Menu Selection Number:
```

Figure 17-1 Menu 24 — System Maintenance

17.1 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyWALL. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

Step 1. Enter number 24 to go to **Menu 24 - System Maintenance**.

Step 2. In this menu, enter 1 to open **System Maintenance - Status**.

Step 3. There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

```
                    Menu 24.1 - System Maintenance - Status          23:10:28
                                                                Sat. Jan. 01, 2000
Port    Status         TxPkts   RxPkts     Cols       Tx B/s    Rx B/s     Up Time
WAN     10M/Half            67  289        0          74        64         2:20:56
LAN     10M/Half           299  220        0          74        64         2:20:54



Port:      Ethernet Address       IP Address            IP Mask          DHCP
WAN        00:a0:c5:21:8c:a3      x.y.155.97            255.255.255.0    Client
LAN        00:a0:c5:21:8c:a2      192.168.1.1           255.255.255.0    Server
DMZ        00:a0:c5:ff:01:02          0.0.0.0           0.0.0.0            None
      WLAM 00:00:00:00:00:00

System up Time: 22:11:43

     Name:
     Routing: IP
     ZyNOS F/W Version: V3.50(WC.0)b6 | 10/04/2001
Press Command:

                  COMMANDS: 1-Drop WAN 9-Reset Counters   ESC-Exit
```

Figure 17-2 Menu 24.1 — System Maintenance — Status

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and are meant to be used for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 17-1 System Maintenance — Status Menu Fields

FIELD	DESCRIPTION
Port	This is the WAN or the LAN port.
Status	Shows the port speed and duplex setting if you're using **Ethernet Encapsulation** and **Down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using **PPPoE Encapsulation**.
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.

Table 17-1 System Maintenance — Status Menu Fields

FIELD	DESCRIPTION
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
Ethernet Address	The Ethernet address of the port listed on the left.
IP Address	The IP address of the port listed on the left.
IP Mask	The IP mask of the port listed on the left.
DHCP	The DHCP setting of the port listed on the left.
System up Time	The total time the ZyWALL has been on.
Name	This is the ZyWALL's system name + domain name assigned in menu 1. e.g., System Name= xxx; Domain Name= baboo.mickey.com. Name= xxx.baboo.mickey.com
Routing	This field refers to the routing protocol used.
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

17.2 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

Step 1. Enter 24 to go to **Menu 24 – System Maintenance**.

Step 2. Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.

Step 3. From this menu you have two choices as shown in the next figure:

```
Menu 24.2 - System Information and Console Port Speed

      1. System Information
      2. Console Port Speed



            Please enter selection:
```

Figure 17-3 Menu 24.2 — System Information and Console Port Speed

17.2.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

```
Menu 24.2.1 - System Maintenance - Information
       Name:
       Routing: IP
       ZyNOS F/W Version: V3.50(WC.0)b6 | 10/04/2001



       LAN
         Ethernet Address: 00:a0:c5:84:09:32
         IP Address: 192.168.1.1
         IP Mask: 255.255.255.0
         DHCP: Server



            Press ESC or RETURN to Exit
```

Figure 17-4 Menu 24.2.1 — System Maintenance — Information

Table 17-2 Fields in System Maintenance — Information

FIELD	DESCRIPTION
Name	This is the ZyWALL's system name + domain name assigned in menu 1. Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the version of ZyXEL's Network Operating System software.
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your ZyWALL.

Table 17-2 Fields in System Maintenance — Information

FIELD	DESCRIPTION
IP Address	This is the IP address of the ZyWALL in dotted decimal notation.
IP Mask	This shows the IP mask of the ZyWALL.
DHCP	This field shows the DHCP setting of the ZyWALL.
When finished viewing, press [ESC] or [ENTER] to exit.	

17.2.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your ZyWALL supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Use [SPACE BAR] to select the desired speed in menu 24.2.2, as shown below.

```
        Menu 24.2.2 - System Maintenance - Change Console Port Speed

                  Console Port Speed: 115200




               Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 17-5 Menu 24.2.2 — System Maintenance — Change Console Port Speed

17.3 Log and Trace

There are two logging facilities in the ZyWALL. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

17.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

Step 1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.

Step 2. From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.

Step 3. Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the ZyWALL finishes displaying, you will have the option to clear the error log.

```
                Menu 24.3 - System Maintenance - Log and Trace

        1. View Error Log
        2. UNIX Syslog

        4. Call-Triggering Packet


                          Please enter selection
```

Figure 17-6 Menu 24.3 — System Maintenance — Log and Trace

Examples of typical error and information messages are presented in the figure below.

```
 0 Wed Aug 22 21:23:26 2001 PP17  INFO  getDateTime fail: no server available
 1 Wed Aug 22 21:23:26 2001 PP17  INFO  adjtime task pause 60 seconds
 2 Wed Aug 22 21:23:54 2001 PINI  INFO  SMT Session Begin
 3 Wed Aug 22 21:24:26 2001 PP0d  INFO  No DNS server available
 4 Wed Aug 22 21:24:26 2001 PP17  WARN  Wrong domain name
 5 Wed Aug 22 21:24:26 2001 PP0d  INFO  No DNS server available
 6 Wed Aug 22 21:24:26 2001 PP17  INFO  Last errorlog repeat 8 Times
 7 Wed Aug 22 21:24:26 2001 PP17  INFO  getDateTime fail: no server available
 8 Wed Aug 22 21:24:26 2001 PP17  INFO  adjtime task pause 1 day
10 Thu Aug 23 08:26:59 2001 PINI -WARN  SNMP TRAP 0: cold start
11 Thu Aug 23 08:26:59 2001 PINI  INFO  main: init completed
12 Thu Aug 23 08:27:04 2001 PP17  INFO  adjtime task pause 1 day
13 Thu Aug 23 08:27:28 2001 PINI  INFO  SMT Session Begin
14 Thu Aug 23 08:27:40 2001 PINI  WARN  system name is not configured
15 Thu Aug 23 08:27:41 2001 PP0d  INFO  LAN promiscuous mode <0>
16 Thu Aug 23 08:32:40 2001 PINI  INFO  SMT Session End
17 Thu Aug 23 08:33:07 2001 PINI  INFO  SMT Session Begin
18 Thu Aug 23 09:01:12 2001 PINI  INFO  SMT Session End
19 Thu Aug 23 09:02:09 2001 PINI  INFO  SMT Session Begin
```

Figure 17-7 Examples of Error and Information Messages

17.3.2 UNIX Syslog

The ZyWALL uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog and Accounting**, as shown next.

```
Menu 24.3.2 - System Maintenance - UNIX Syslog and Accounting

    Syslog:
    Active= No
    Syslog IP Address= ?
    Log Facility= Local 1

    Types:
    CDR= No
    Packet Triggered= No
    Filter log= No
    PPP log= No

    Firewall log= No


    Press ENTER to Confirm or ESC to Cancel
```

Figure 17-8 Menu 24.3.2 — System Maintenance — UNIX Syslog

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 17-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Press [SPACE BAR] to turn syslog on or off.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more details.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.

Table 17-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
Filter log	No filters are logged when this field is set to **No**. Filters with the individual filter Log Filter field set to **Yes** (Menu 21.x.x).) are logged when this field is set to **Yes**.
PPP log	PPP events are logged when this field is set to **Yes**.
Firewall log	When set to **Yes**, the ZyWALL sends the firewall log to a syslog server.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your ZyWALL sends five types of syslog messages. Some examples (not all ZyWALL specific) of these syslog messages with their message formats are shown next:

1. CDR

CDR Message Format

SdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String);

String = board xx line xx channel xx, call xx, str

board = the hardware board ID

line = the WAN ID in a board

Channel = channel ID within the WAN

call = the call reference number which starts from 1 and increments by 1 for each new call

str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)

L02 Tunnel Connected(L2TP)

C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)

L02 Call Terminated

C02 Call Terminated

Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002

Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002

Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated

2. Packet triggered

Packet triggered Message Format

sdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, String);

String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x

Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)

Data: We will send forty-eight Hex characters to the server

Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374

Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4

Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=450000282401400001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3. Filter log

Filter log Message Format

SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).

Src: Source Address

Dst: Destination Address

prot: Protocol (“TCP”,”UDP”,”ICMP”)

spo: Source port

dpo: Destination port

Mar 03 10:39:43 202.132.155.97 ZyXEL:

GEN[ffffffffffnordff0080] }S05>R01mF

Mar 03 10:41:29 202.132.155.97 ZyXEL:

GEN[00a0c5f502fnord010080] }S05>R01mF

Mar 03 10:41:34 202.132.155.97 ZyXEL:

IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF

Mar 03 11:59:20 202.132.155.97 ZyXEL:

GEN[00a0c5f502fnord010080] }S05>R01mF

Mar 03 12:00:52 202.132.155.97 ZyXEL:

GEN[ffffffffffff0080] }S05>R01mF

Mar 03 12:00:57 202.132.155.97 ZyXEL:

GEN[00a0c5f502010080] }S05>R01mF

Mar 03 12:01:06 202.132.155.97 ZyXEL:

IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

4. PPP log

PPP Log Message Format
sdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing

5. Firewall log

Firewall Log Message Format
sdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf); buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol (“TCP”,”UDP”,”ICMP”, ”IGMP”, ”GRE”, ”ESP”)
rule: <a,b> where a means "set" number; b means "rule" number.
action: nothing(N) block (B) forward (F)
08-01-2000 11:48:41 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.80 :137 ->172.21.1.80 :137 |UDP|default permit:<2,0>|B
08-01-200011:48:41 Local1.Notice 192.168.10.10 RAS: FW 192.168.77.88 :520 ->192.168.77.88 :520 |UDP|default permit:<2,0>|B
08-01-2000 11:48:39 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.50 ->172.21.1.50 |IGMP<2>|default permit:<2,0>|B
08-01-2000 11:48:39 Local1.Notice 192.168.10.10 RAS: FW 172.21.1.25 ->172.21.1.25 |IGMP<2>|default permit:<2,0>|B

17.3.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
 Frame Type:

   IP Header:
     IP Version               = 4
     Header Length            = 20
     Type of Service          = 0x00 (0)
     Total Length             = 0x002C (44)
     Identification            = 0x0002 (2)
     Flags                    = 0x00
     Fragment Offset          = 0x00
     Time to Live             = 0xFE (254)
     Protocol                 = 0x06 (TCP)
     Header Checksum          = 0xFB20 (64288)
     Source IP                = 0xC0A80101 (192.168.1.1)
     Destination IP           = 0x00000000 (0.0.0.0)

   TCP Header:
     Source Port              = 0x0401 (1025)
     Destination Port         = 0x000D (13)
     Sequence Number          = 0x05B8D000 (95997952)
     Ack Number               = 0x00000000 (0)
     Header Length            = 24
     Flags                    = 0x02 (....S.)
     Window Size              = 0x2000 (8192)
     Checksum                 = 0xE06A (57450)
     Urgent Ptr               = 0x0000 (0)
     Options                  =
         0000: 02 04 02 00

   RAW DATA:
     0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.........  ....
     0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  ................
     0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

Figure 17-9 Call-Triggering Packet Example

17.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyWALL to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next.

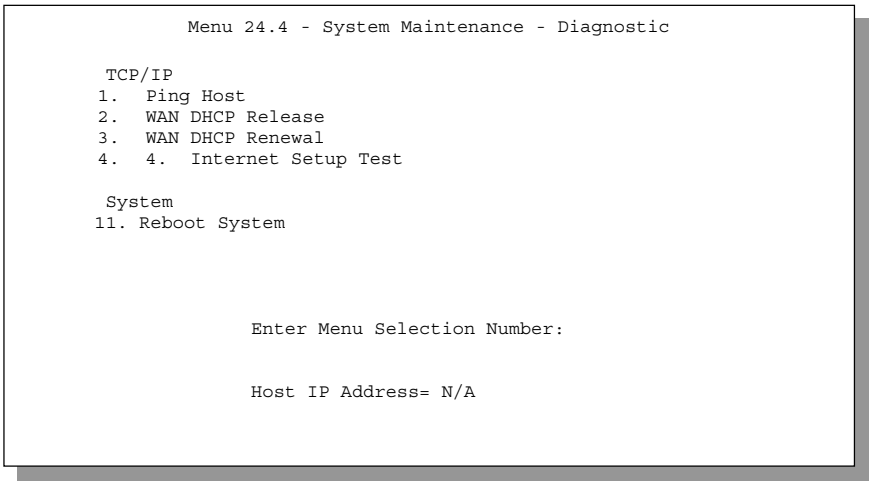


Figure 17-10 Menu 24.4 — System Maintenance — Diagnostic

Follow the procedure below to get to **Menu 24.4 - System Maintenance – Diagnostic.**

Step 1. From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

Step 2. From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

17.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 17-11*. LAN DHCP has already been discussed. The ZyWALL can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, i.e., you have a static IP. The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

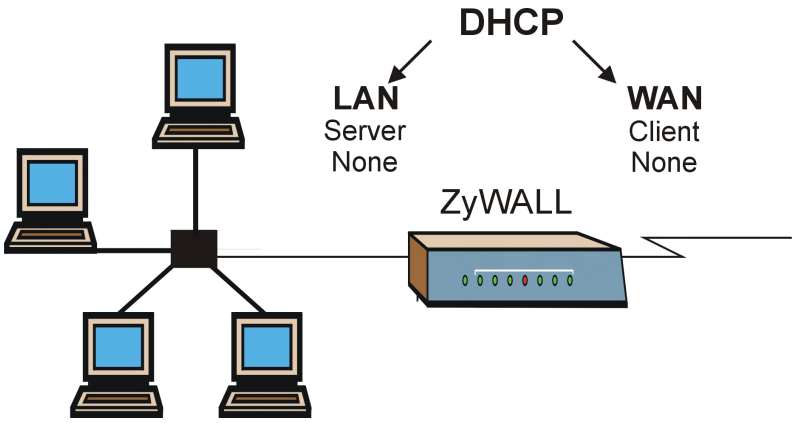


Figure 17-11 WAN & LAN DHCP

The following table describes the diagnostic tests available in menu 24.4 for your ZyWALL and associated connections.

Table 17-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address** field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet Setup. You can also test the Internet Setup in **Menu 4 - Internet Access**. Please refer to the *Internet Access* chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the ZyWALL.
Host IP Address=	If you entered 1 in the **Host IP Address** field above, then enter the IP address of the machine you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

Chapter 18
Firmware and Configuration Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

18.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a “rom” filename extension. Once you have customized the ZyWALL's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the “ras” file) is the system firmware and has a “bin” filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```
This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyWALL.

```
ftp> get rom-0 config.cfg
```
This is a sample FTP session saving the current configuration to the computer file “config.cfg”.

If your (t)ftp client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyWALL only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyWALL and the external filename refers to the filename not on the ZyWALL, that is, on your computer, local network or FTP site and so the name (but not the extension) will vary. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that

you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 18-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the ZyWALL. Uploading the rom-0 file replaces the entire ROM file system, including your ZyWALL configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the ZyWALL.

18.2 Backup Configuration

The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files (see *section 18.1*).

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyWALL to the computer, while upload means from your computer to the ZyWALL.

18.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

```
              Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current System configuration to
   your workstation.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your System manual.


Press ENTER to Exit:
```

Figure 18-1 Telnet in Menu 24.5

18.2.2 Using the FTP Command from the Command Line

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “get” to transfer files from the ZyWALL to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the FTP prompt.

18.2.3 Example of FTP Commands from the Command Line

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 18-2 FTP Session Example

18.2.4 GUI-Based FTP Clients

The following table describes some of the commands that you may see in GUI-Based FTP clients.

Table 18-2 General Commands for GUI-Based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

18.2.5 TFTP and FTP over WAN Will Not Work When

- Telnet service is disabled in menu 24.11.
- A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block Telnet service.
- The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the Telnet session immediately.

- There is an SMT console session running.
- The firewall is active. The default firewall policies block all traffic from the WAN, so to enable TFTP over the WAN, you must turn the firewall off (menu 21.2) or create a firewall rule to allow TFTP from the WAN.

18.2.6 Backup Configuration Using TFTP

The ZyWALL supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

Step 1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyWALL to the computer and “binary” to set binary transfer mode.

18.2.7 TFTP Command Example

The following is an example TFTP command:

```
TFTP [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL IP address, “get” transfers the file source on the ZyWALL (rom-0 name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

18.2.8 GUI-Based TFTP Clients

The following table describes some of the fields that you may see in GUI-Based TFTP clients.

Table 18-3 General Commands for GUI-Based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyWALL. 192.168.1.1 is the ZyWALL’s default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the ZyWALL and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyWALL. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 18.2.5* to read about configurations that disallow TFTP and FTP over WAN.

18.2.9 Backup Via Console Port

Backup configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.5 and enter “y” at the following screen.

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 18-3 System Maintenance — Backup Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

Figure 18-4 System Maintenance — Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

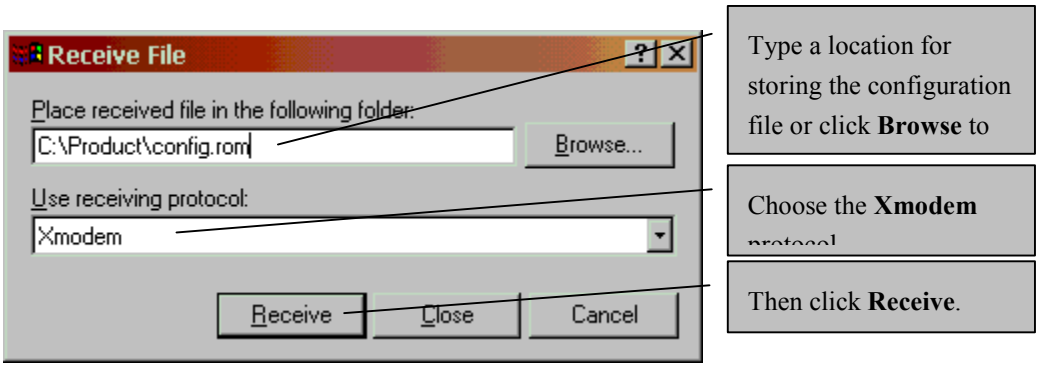


Figure 18-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

Figure 18-6 Successful Backup Confirmation Screen

18.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred methods for restoring your current computer configuration to your ZyWALL since it is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYWALL. WHEN THE RESTORE CONFIGURATION PROCESS IS COMPLETE, THE ZYWALL WILL AUTOMATICALLY RESTART.

18.3.1 Restore Using FTP or TFTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

```
              Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow the
procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
   SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-spt is the
   remote file name on the router. This restores the configuration to
   your router.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your System manual.


Press ENTER to Exit:
```

Figure 18-7 Telnet into Menu 24.6

18.3.2 Procedure To Restore Using FTP

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Find the “rom” file (on your computer) that you want to restore to your ZyWALL.

Step 7. Use "put" to transfer files from the Prestige to the computer, for example, "put config.rom rom-0" transfers the configuration file "config.rom" on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.

Step 8. Enter “quit” to exit the FTP prompt. The ZyWALL will automatically restart after a successful restore process.

18.3.3 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figure 18-8 Restore Using FTP or TFTP Session Example

Refer to *section 18.2.5* to read about configurations that disallow TFTP and FTP over WAN.

18.3.4 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.6 and enter “y” at the following screen.

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 18-9 System Maintenance — Restore Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCCC
```

Figure 18-10 System Maintenance — Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

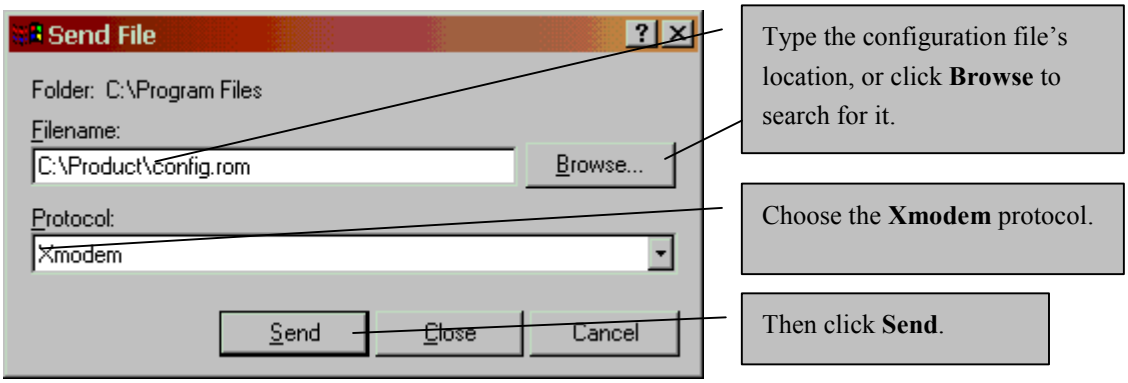


Figure 18-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the ZyWALL and return to the SMT menu.

```
Save to ROM
Hit any key to start system reboot.
```

Figure 18-12 Successful Restoration Confirmation Screen

18.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

WARNING!
DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYWALL.

18.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyWALL, you will see the following screens for uploading firmware and the configuration file using FTP.

```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.


For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


Press ENTER to Exit:
```

Figure 18-13 Telnet Into Menu 24.7.1 — Upload System Firmware

18.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

```
          Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

Figure 18-14 Telnet Into Menu 24.7.2 — System Maintenance

To upload the firmware and the configuration file, follow these examples

18.4.3 FTP File Upload Command from the Command Line Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open”, followed by a space and the IP address of your ZyWALL.

Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter your password as requested (the default is “1234”).

Step 5. Enter “bin” to set transfer mode to binary.

Step 6. Use “put” to transfer files from the computer to the ZyWALL, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyWALL and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

Step 7. Enter “quit” to exit the FTP prompt.

18.4.4 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 18-15 FTP Session Example of Firmware File Upload

More commands (found in GUI-Based FTP clients) are listed earlier in this chapter.

Refer to *section 18.2.5* to read about configurations that disallow TFTP and FTP over WAN.

18.4.5 TFTP File Upload

The ZyWALL also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

Step 1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the ZyWALL in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyWALL to the computer, “put” the other way around, and “binary” to set binary transfer mode.

18.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
TFTP [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

Commands that you may see in GUI-Based TFTP clients are listed earlier in this chapter.

18.4.7 Uploading Via Console Port

FTP is the preferred methods for uploading firmware to your ZyWALL. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyWALL via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

18.4.8 Uploading a Firmware File Via Console Port

Step 1. Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload System Firmware**, then follow the instructions as shown in the following screen.

```
            Menu 24.7.1 - System Maintenance - Upload System Firmware


To upload System firmware:

1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   router.

Warning: Proceeding with the upload will erase the current router
firmware.
                Do You Wish To Proceed:(Y/N)
```

Figure 18-16 Menu 24.7.1 as seen using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

18.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

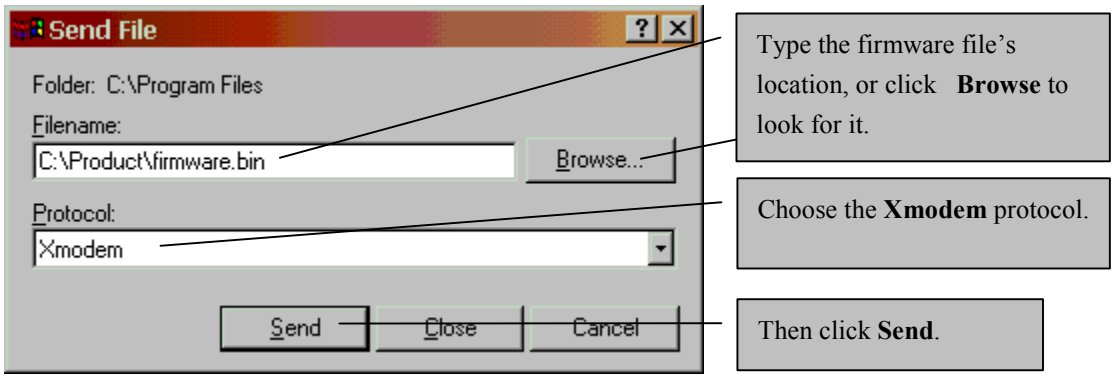


Figure 18-17 Example Xmodem Upload

After the firmware upload process has completed, the ZyWALL will automatically restart.

18.4.10 Uploading a Configuration File Via Console Port

Step 1. Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File


To upload System configuration file:

1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   router.

Warning:
1. Proceeding with the upload will erase the current
   configuration file.
2. The router's console port speed (Menu 24.2.2) may change
   when it is restarted; please adjust your terminal's speed
   accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
   port speed will be reset to 9600 bps and the password to
   "1234".
                  Do You Wish To Proceed:(Y/N)
```

Figure 18-18 Menu 24.7.2 as seen using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 3. Enter “atgo” to restart the ZyWALL.

18.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

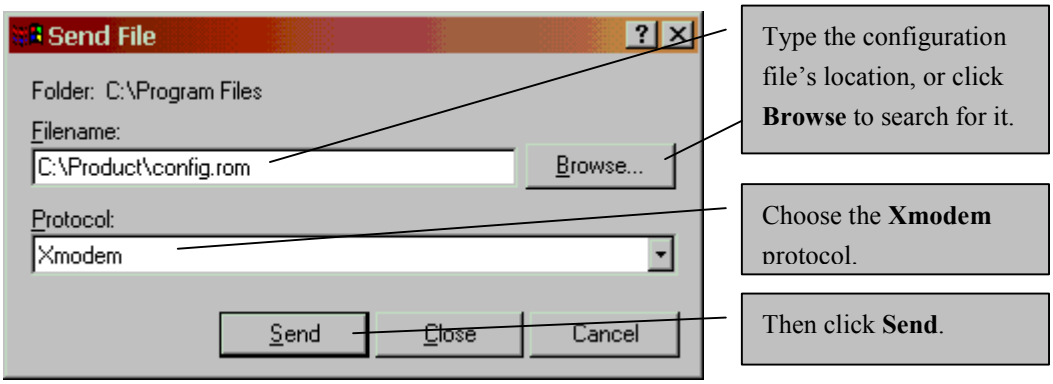


Figure 18-19 Example Xmodem Upload

After the configuration upload process has completed, restart the ZyWALL by entering "atgo".

Chapter 19
System Maintenance & Information

This chapter leads you through SMT menus 24.8 to 24.11.

19.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be either by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or the zyxel.com web site for more detailed information on CI commands. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "exit" to return to the SMT main menu when finished.

```
                    Menu 24 - System Maintenance

                        1.  System Status
                        2.  System Information and Console Port Speed
                        3.  Log and Trace
                        4.  Diagnostic
                        5.  Backup Configuration
                        6.  Restore Configuration
                        7.  Firmware Update
                        8.  Command Interpreter Mode
                        9.  Call Control
                        10. Time and Date Setting
                        11. Remote Management Setup



                         Enter Menu Selection Number:
```

Figure 19-1 Command Mode in Menu 24

```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
poe             pptp               ip           ipsec
ppp           bridge              hdap
ras>
```

Figure 19-2 Valid Commands

19.2 Call Control Support

The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

```
                Menu 24.9 - System Maintenance - Call Control


Budget Management
Call History



Enter Menu Selection Number:
```

Figure 19-3 Call Control

19.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

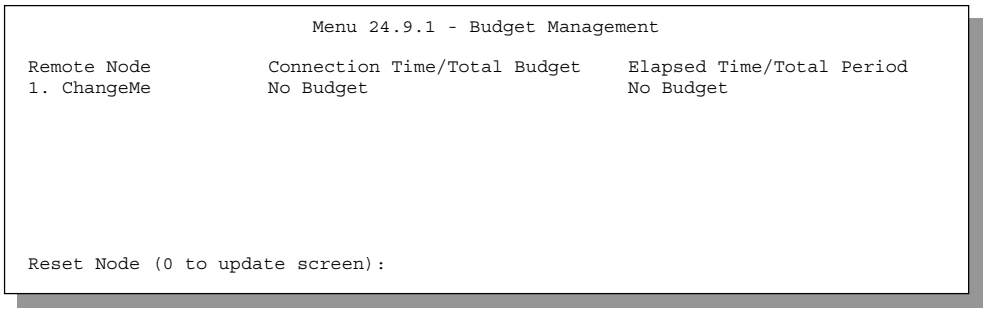


Figure 19-4 Budget Management

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 19-1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter “0” to update the screen or press [ESC] to return to the previous screen.		

19.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

```
                          Menu 24.9.2 - Call History

    Phone Number    Dir    Rate      #call        Max         Min         Total
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
Enter Entry to Delete(0 to exit):
```

Figure 19-5 Call History

Table 19-2 Call History Fields

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or “”0” to exit.	

19.3 Time and Date Setting

The ZyWALL has a Real Time Chip (RTC) that keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

```
                    Menu 24 - System Maintenance

                  1.     System Status
                  2.     System Information and Console Port Speed
                  3.     Log and Trace
                  4.     Diagnostic
                  5.     Backup Configuration
                  6.     Restore Configuration
                  7.     Upload Firmware
                  8.     Command Interpreter Mode
                  9.     Call Control
                  10.    Time and Date Setting
                  11.    Remote Management Setup

Enter Menu Selection Number:
```

Figure 19-6 Menu 24 — System Maintenance

Then enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your ZyWALL as shown in the following screen.

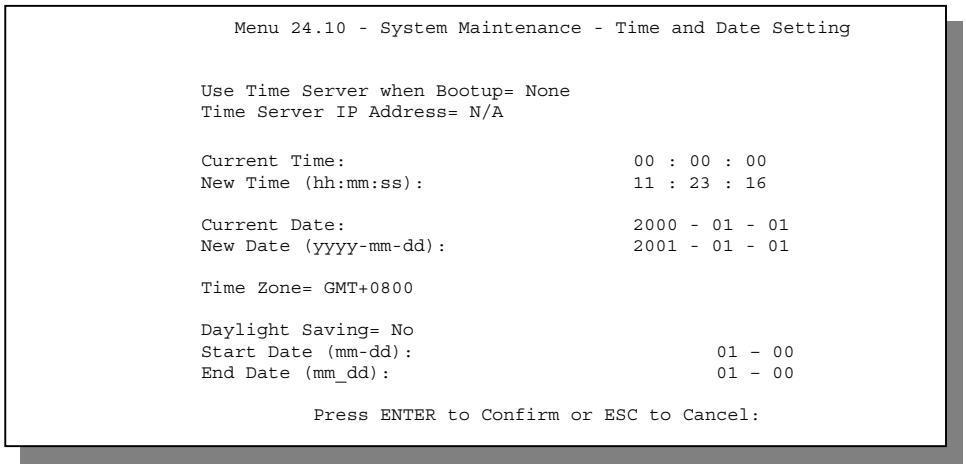

Menu 24.10 - System Maintenance - Time and Date Setting
Use Time Server when Bootup= None
Time Server IP Address= N/A
Current Time: 00 : 00 : 00
New Time (hh:mm:ss): 11 : 23 : 16
Current Date: 2000 - 01 - 01
New Date (yyyy-mm-dd): 2001 - 01 - 01
Time Zone= GMT+0800
Daylight Saving= No
Start Date (mm-dd): 01 - 00
End Date (mm_dd): 01 - 00
Press ENTER to Confirm or ESC to Cancel:

Figure 19-7 Menu 24.10 System Maintenance — Time and Date Setting

Table 19-3 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the ZyWALL. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None** is the default value. Enter the time manually. Each time you turn on the ZyWALL, the time and date will be reset to 2000-1-1 0:0:0.
Time Server IP Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] to set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 19-3 Time and Date Setting Fields

FIELD	DESCRIPTION
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

19.3.1 Resetting the Time

The ZyWALL resets the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the ZyWALL starts up, if there is a time server configured in menu 24.10.

iii. 24-hour intervals after starting.

Chapter 20
Remote Management

This chapter covers remote management found in SMT menu 24.11.

20.1 Telnet

The only way to configure the ZyWALL for remote management is through an SMT session using the console port. Once your ZyWALL is configured, you can use telnet to configure it remotely as shown next.

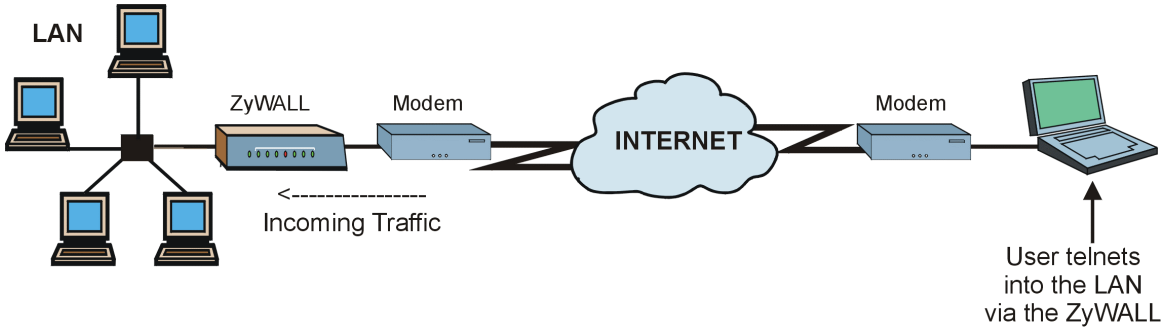


Figure 20-1 Telnet Configuration on a TCP/IP Network

20.2 FTP

You can upload and download ZyWALL firmware and configuration files using FTP - please see *Chapter 18* for details. To use this feature, your computer must have an FTP client.

20.3 Web

You can use the ZyWALL's embedded web configurator for configuration and file management. See the *Using the ZyWALL Web Configurator* chapter for an introduction to the web configurator.

20.4 Remote Management

Remote management control is for managing Telnet, Web and FTP services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your ZyWALL from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable)

Choosing WAN only **or** ALL **(LAN & WAN) automatically creates a hole in the firewall for the server type specified.**

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

```
                    Menu 24.11 - Remote Management Control

      TELNET Server:
        Server Port = 23                  Server Access = LAN only
        Secured Client IP = 0.0.0.0

      FTP Server:
        Server Port = 21                  Server Access = LAN only
        Secured Client IP = 0.0.0.0

      Web Server:
        Server Port = 80                  Server Access = LAN only
        Secured Client IP = 0.0.0.0



                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 20-2 Menu 24.11 – Remote Management Control

Table 20-1 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
TELNET Server FTP Server Web Server	These read-only labels denote the kind of server that you may remotely manage.	
Server Port	You may change the service port number for corresponding services in this field.	23
Server Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.	**LAN Only** (default)
Secured Client IP	The default value for **Secured Client IP** is 0.0.0.0, which means you don't care which host is trying to use a service (Telnet, FTP or Web). If you enter an IP address in this field, the ZyWALL will check if the client IP address matches the value here when a (Telnet, FTP or Web) session is up. If it does not match, the ZyWALL will disconnect the session immediately. If the **Server Access** field is set to **Disable**, then this field is **N/A**.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

20.4.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session of the same type (web, FTP or Telnet) running. You may only have one remote management session of the same type running at one time.

6. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

20.5 Remote Management and NAT

When NAT is enabled:

- Use the ZyWALL's WAN IP address when configuring from the WAN.
- Use the ZyWALL's LAN IP address when configuring from the LAN.

20.6 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your ZyWALL will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Part V:

Call Scheduling and VPN/IPSec

Part V provides information about Call Scheduling and VPN/IPSec.

Chapter 21
Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

21.1 Introduction

The call scheduling feature allows the ZyWALL to manage a remote node and dictate when a remote node should be called and for how long. This feature is to the scheduler in a video cassette recorder (you can record programs you want during a time that is specified by you). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.

```
                        Menu 26 - Schedule Setup

  Schedule                              Schedule
  Set #         Name                    Set #          Name
  ------        --------------------    ------         ----------------
  1             ________________        7              --
  2             ________________        8              ________________
  3             ________________        9              ________________
  4             ________________        10             ________________
  5             ________________        11             ________________
  6             ________________        12             ________________
                                                       ________________
                      Enter Schedule Set Number to Configure=

                      Edit Name=

                      Press ENTER to Confirm or ESC to Cancel:
```

Figure 21-1 Menu 26 - Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the ZyWALL, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to twelve schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] or [DELETE] in the Edit Name **field.**

To setup a schedule set select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

```
                        Menu 26.1 - Schedule Set Setup

                Active= Yes
                Start Date(yyyy/mm/dd) = 2000 - 01 - 01
                How Often= Once
                Once:
                  Date(yyyy/mm/dd)= 2000 - 01 - 01
                Weekdays:
                  Sunday= N/A
                  Monday= N/A
                  Tuesday= N/A
                  Wednesday= N/A
                  Thursday= N/A
                  Friday= N/A
                  Saturday= N/A
                Start Time (hh:mm)= 00 : 00
                Duration (hh:mm)= 00 : 00
                Action= Forced On

                          Press ENTER to Confirm or ESC to Cancel:
      Press Space Bar to Toggle
```

Figure 21-2 Schedule Set Setup

If a connection has been already established, your ZyWALL will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 21-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTION
Active	Press [SPACE BAR] to toggle between **Yes** and **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes/No**
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] to toggle between **Once** and **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes	**Once/Weekly**

Table 21-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	OPTION
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] to toggle between **Once** and **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once/Weekly**
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	Maximum duration
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field.	**Forced On**
	Forced Down means that the connection is blocked whether or not there is a demand call on the line.	**Forced Down**
	Enable Dial-On-Demand means that this schedule permits a demand call on the line.	**Enable Dial-On-Demand**
	Disable Dial-On-Demand means that this schedule prevents a demand call on the line.	**Disable Dial-On-Demand**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter **11** from the Main Menu and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

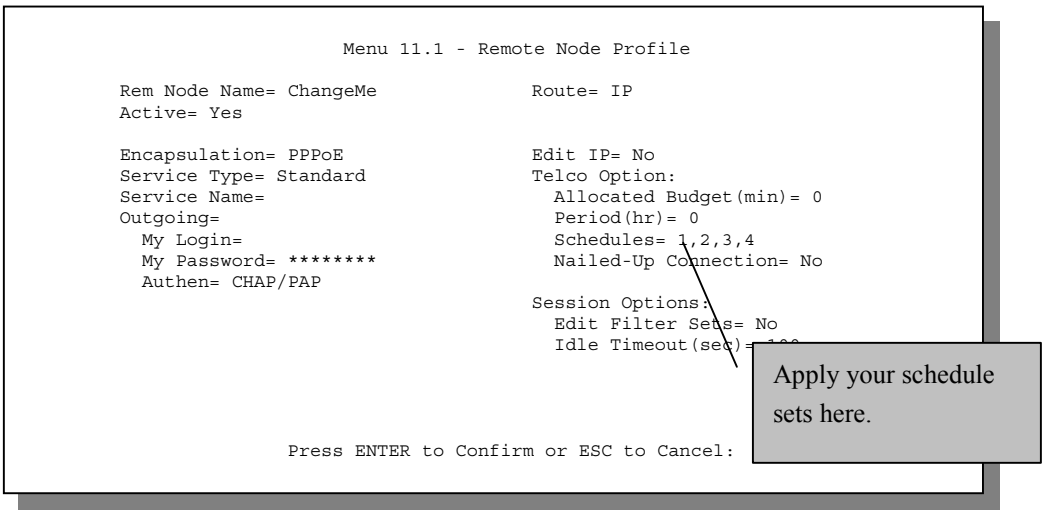


Figure 21-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to 4 schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

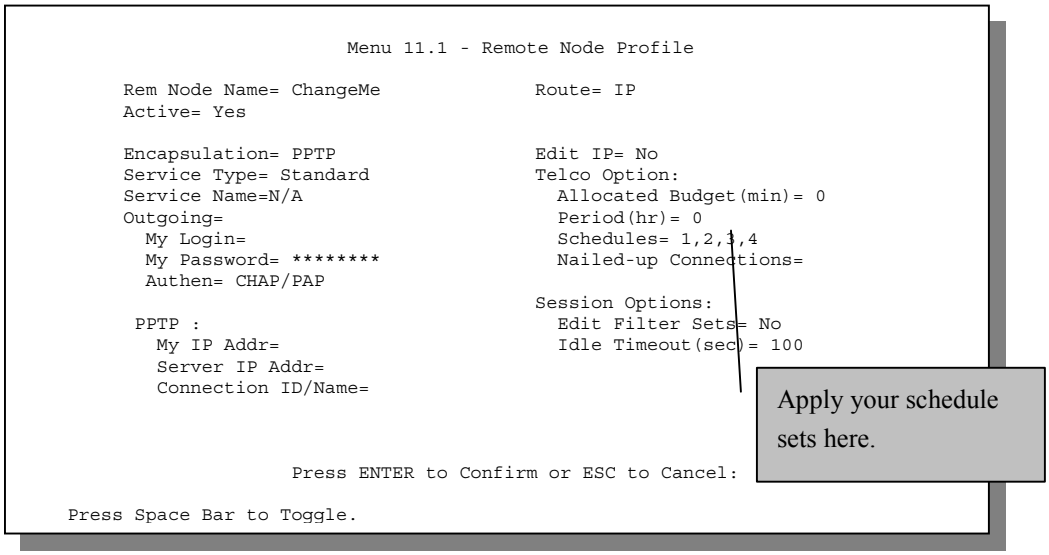


Figure 21-4 Applying Schedule Set(s) to a Remote Node (PPTP)

Chapter 22
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

22.1 Introduction

22.1.1 VPN

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

22.1.2 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

22.1.3 Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

22.1.4 Other Terminology

- **Encryption**

  Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

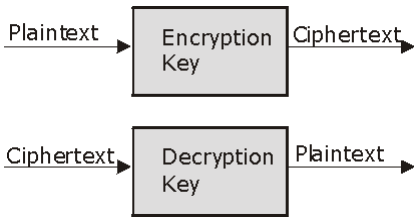


Figure 22-1 Encryption and Decryption

- **Data Confidentiality**

  The IPSec sender can encrypt packets before transmitting them across a network.

- **Data Integrity**

  The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

- **Data Origin Authentication**

  The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

22.1.5 VPN Applications

The ZyWALL 50 supports 50 Security Associations (SAs).

- **Linking Two or More Private Networks Together**

  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- **Accessing Network Resources When NAT Is Enabled**

  When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

- **Unsupported IP Applications**

  A VPN tunnel may be created to add support for unsupported emerging IP applications.

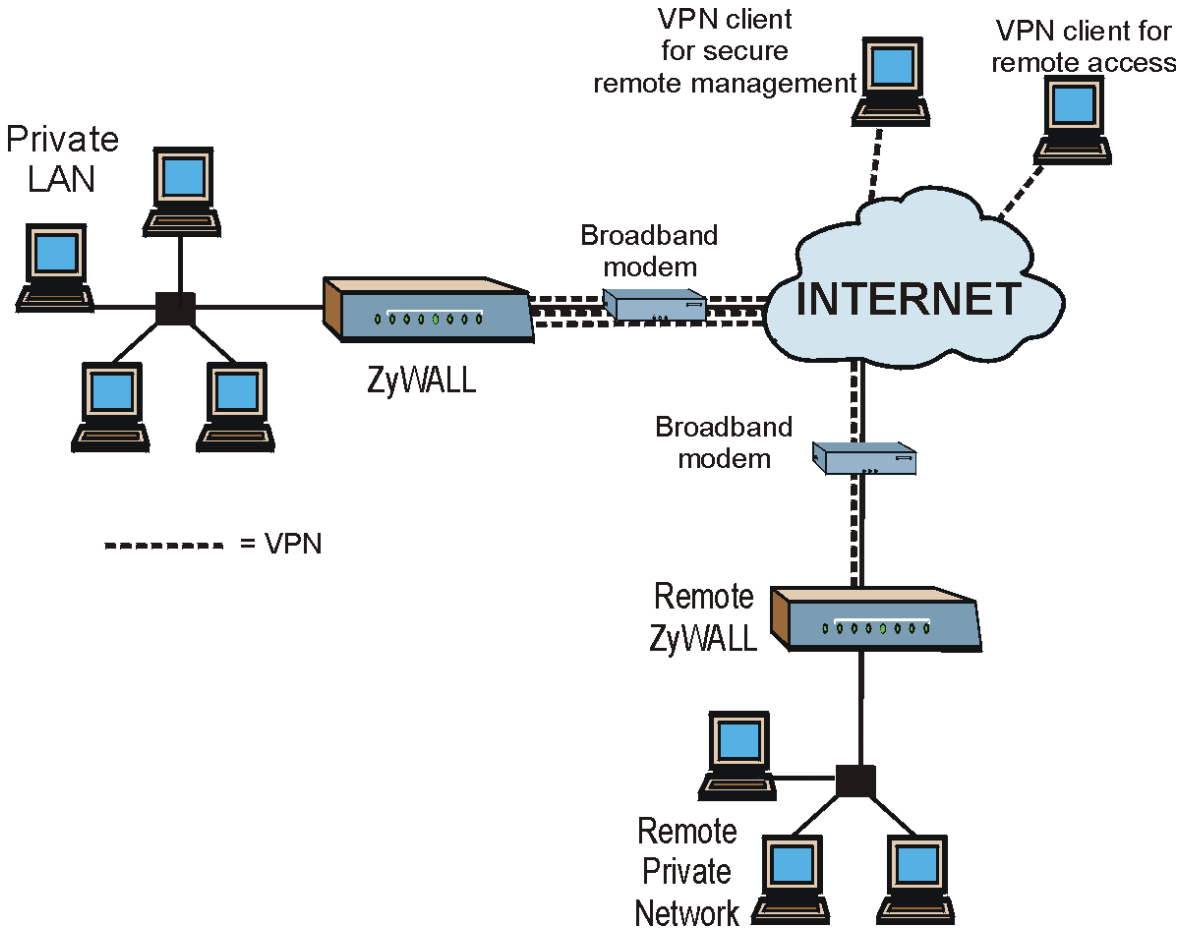


Figure 22-2 VPN Application

22.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

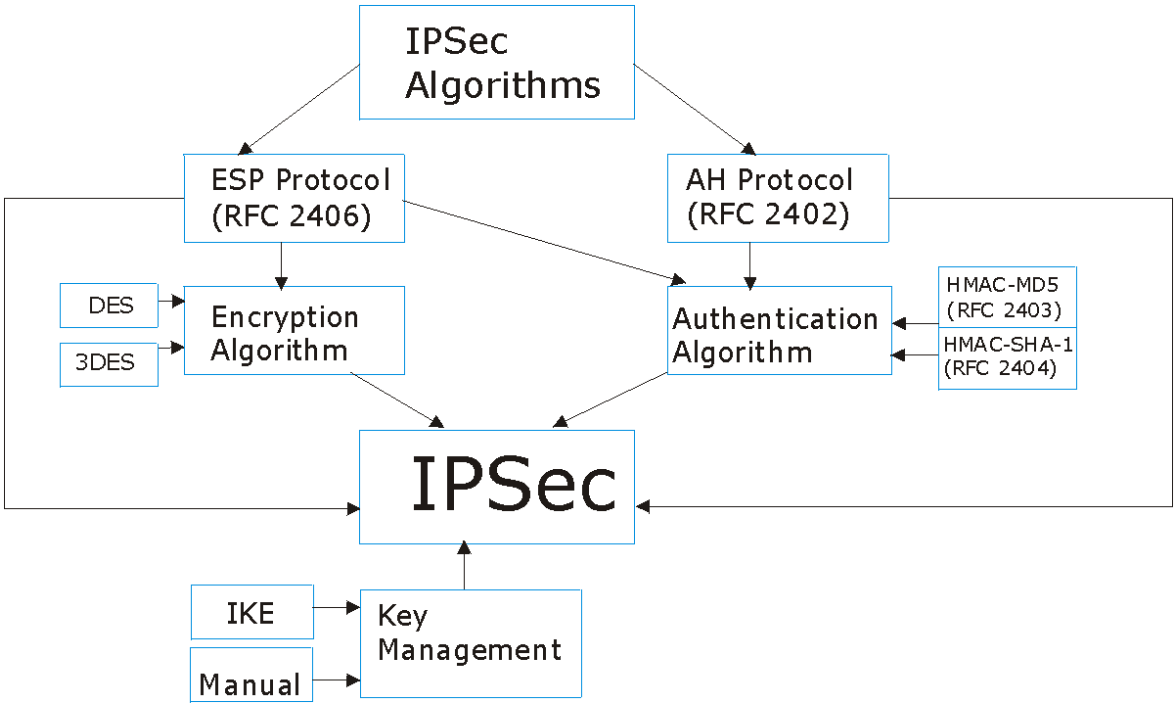


Figure 22-3 IPSec Architecture

22.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).
The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.
The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see *section 23.2* for more information.

22.2.2 Key Management

Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN. Please see *sections 23.4* and *23.5* for more information.

22.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

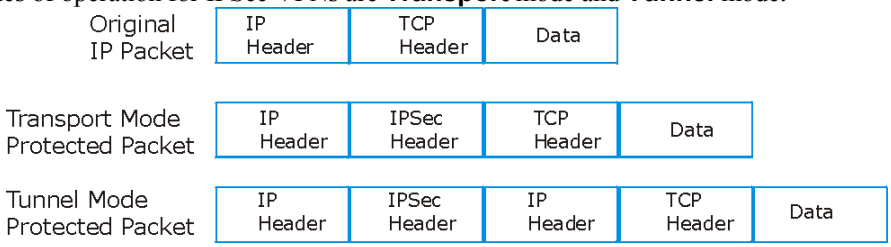


Figure 22-4 Transport and Tunnel Mode IPSec Encapsulation

22.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.
With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

22.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

22.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyWALL.
NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.
IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.
Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.
Transport mode **ESP** with authentication is not compatible with NAT.

Table 22-1 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

Chapter 23
VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

23.1 VPN/IPSec Setup

The VPN/IPSec main SMT menu has three main submenus.

1. Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.
2. **Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.
3. View the IPSec connection log in menu 27.4. This menu is also useful for troubleshooting.

This is an overview of the VPN menu tree.

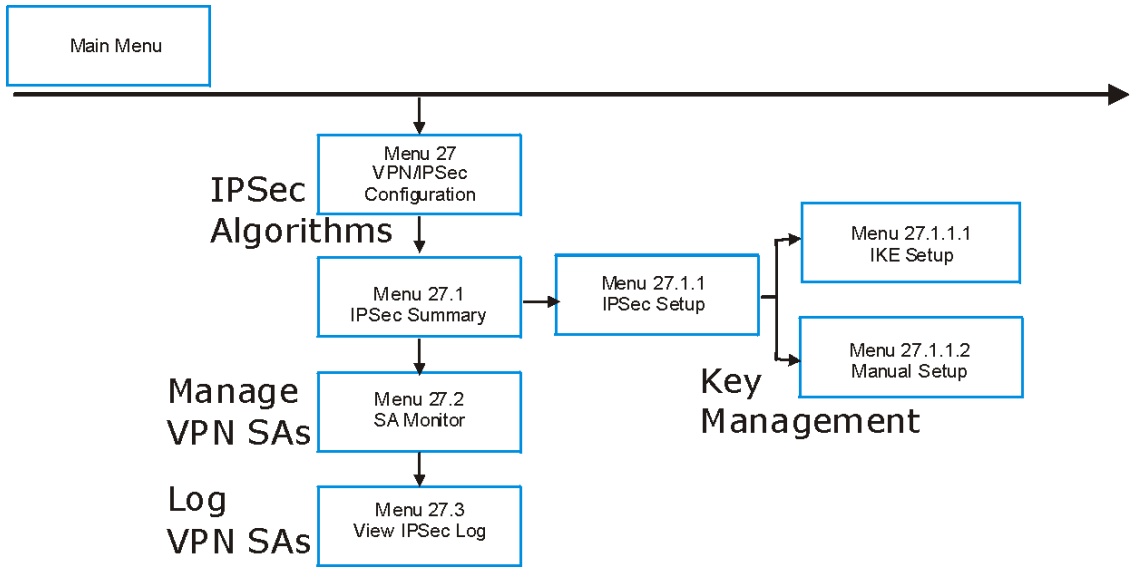


Figure 23-1 VPN SMT Menu Tree

From the main menu, enter 27 to display the first VPN menu (shown next).

```
                    Menu 27 - VPN/IPSec Setup

                1. IPSec Summary
                2. SA Monitor
                3. View IPSec Log




                      Enter Menu Selection Number:
```

Figure 23-2 Menu 27 — VPN/IPSec Setup

23.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

23.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.
In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

23.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.
An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 23-1 AH and ESP

ESP	AH
Select DES for minimal security and 3DES for maximum.	Select MD5 for minimal security and SHA-1 for maximum security.
DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

23.3 IPSec Summary

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

The following figure helps explain the main fields in menu 27.1.

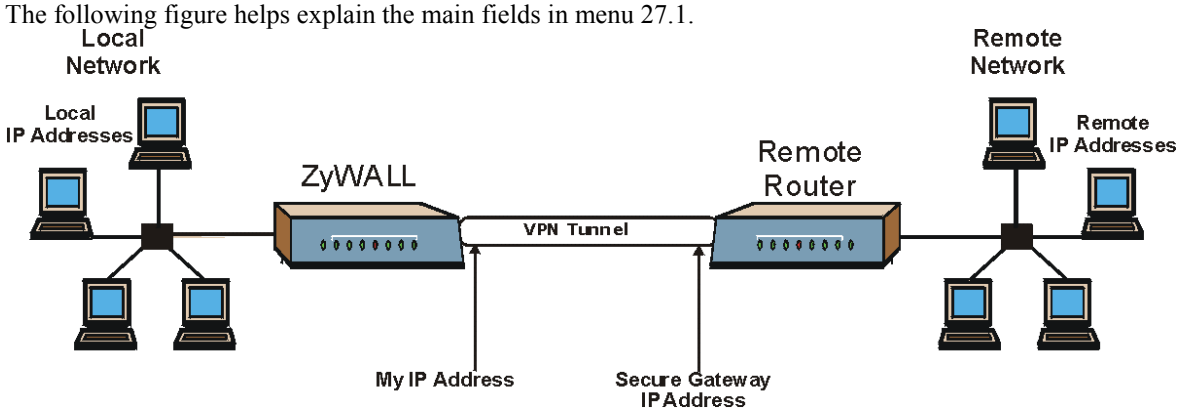


Figure 23-3 IPSec Summary Fields

Local and remote IP addresses must be static. The VPN initiator local IP address range should be identical to the peer remote IP address range. Similarly, the VPN initiator remote IP address range should be identical to the peer local IP address range. If they are not, the connection will fail and this will display in the IPSec log as a local or remote ID failure.

My IP Addr is the (initiator) ZyWALL WAN IP address. If this field is configured as 0.0.0.0, then the ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) to set up the VPN tunnel. If the **My IP Addr** changes after setup, then the VPN tunnel will have to be rebuilt again.
Secure Gateway IP Address is the WAN IP address of the remote IPSec router. Normally it is a static public IP address (for traffic going through the Internet) but if the peer has a dynamic WAN IP address, set this field to 0.0.0.0. This may be useful for telecommuters initiating a VPN tunnel to headquarters where headquarters do not know the WAN IP address of the telecommuter's device. Only the telecommuter may initiate the VPN tunnel in this case. See the following table for an example configuration.

Table 23-2 Telecommuter and HQ Configuration Example

	TELECOMMUTER	HEADQUARTERS
My IP address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address.	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.

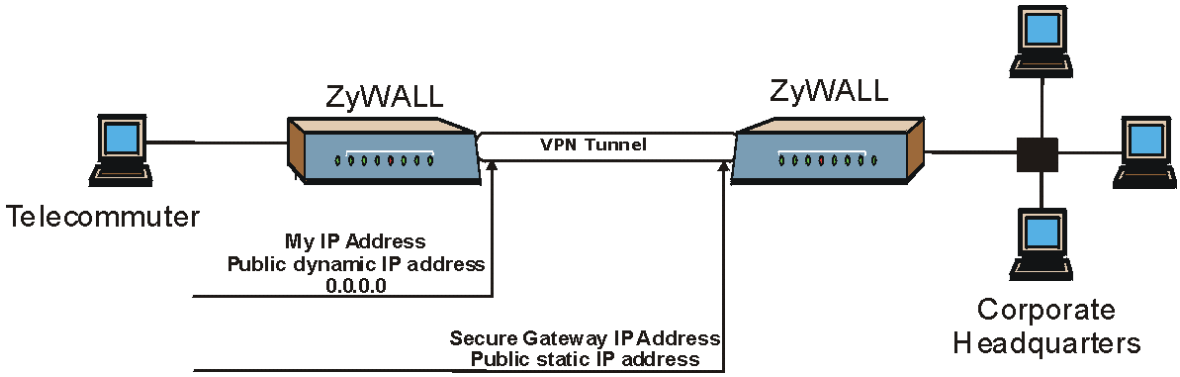


Figure 23-4 Telecommuter's ZyWALL Configuration

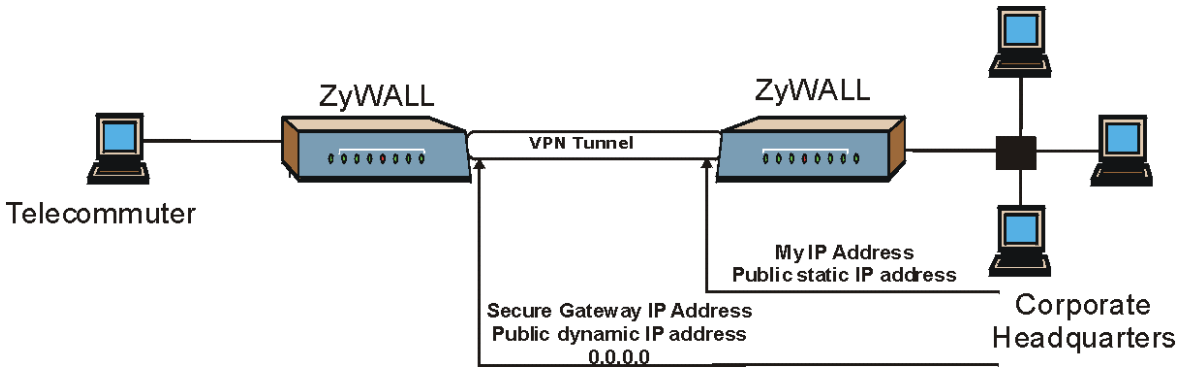


Figure 23-5 HQ ZyWALL Configuration

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using IKE **key negotiation and not** Manual **key negotiation.**

A ZyWALL with Secure Gateway IP Address **set to 0.0.0.0 may receive multiple VPN connection requests using the same VPN rule at the same time.**

```
                        Menu 27.1 - IPSec Summary

#  Name     A  Local Addr Start    - Local Addr End    Encap.   IPSec Algorithms
              Remote Addr Start    - Remote Addr End            Secure GW Address
-  ------   -  -----------------    ---------------     ------   ------------------
1  Taiwan   Y  192.168.1.35        192.168.1.38        Tunnel   ESP DES MD5
              172.16.2.40          172.16.2.46                  193.81.13.2
2  USA      N  192.168.1.39        192.168.1.39        Tunnel   AH SHA1
              172.16.2.50          172.16.2.50                  193.81.13.3
3  China    N  192.168.1.40        192.168.1.42        Tunnel   ESP DES MD5
              172.16.2.55          172.16.2.59                  193.81.13.4
4

5


                Select Command= None                 Select Rule= N/A
                    Press ENTER to Confirm or ESC to Cancel:
```

Figure 23-6 Menu 27.1 — IPSec Summary

Table 23-3 Menu 27.1 — IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
#	This is the VPN policy index number.	1
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.	Taiwan
A	**Y** signifies that this VPN rule is active.	**Y**
Local Addr Start	This is the beginning IP address of the computers on your local network behind your ZyWALL. This must be a static IP address.	192.168.1.35
Local Addr End	This is the end (static) IP address (in a range) of computers on your local network behind your ZyWALL.	192.168.1.38
Remote Addr Start	This is the beginning IP address of the computers on the remote network behind the remote IPSec router. This must be a static IP address.	172.16.2.40
Remote Addr End	This is the end (static) IP address (in a range) of computers on the remote network behind the remote IPSec router.	172.16.2.46
Encap	This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these.	**Tunnel**
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **AH** (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.** Both **AH** and **ESP** increase the ZyWALL's processing requirements and communications latency (delay).	**ESP DES MD5**
Secure Gw Addr	This is the WAN IP address of the IPSec router with which you're making the VPN connection. If the peer has a dynamic WAN IP address, set this field to 0.0.0.0. This may be useful for telecommuters initiating a VPN tunnel to the company network. Only the telecommuter may initiate the VPN tunnel in this case.	Public IP address
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, Delete or **Go To**	**None**

Table 23-3 Menu 27.1 — IPSec Summary

FIELD	DESCRIPTION	EXAMPLE
	commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do not move up in the page list. Use **Go To Rule** to view the page where your desired rule is listed. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].	3
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

You may configure up to 60 IPSec rules in the ZyWALL 50 but only (up to) 50 may be active at any one time.

23.3.1 IPSec Setup

Type an index number and then press [ENTER] to edit the VPN using the menu shown next.

```
                Menu 27.1.1 - IPSec Setup

        Index= 1
        Name= Taiwan
        Active= Yes


        My IP addr= 0.0.0.0
        Secure Gateway IP Addr= 10.12.134.2
        Protocol= 0
        Local:    IP Addr Start= 192.168.1.35   End= 192.168.1.38
                     Port Start= 0              End=N/A
        Remote:   IP Addr Start= 172.16.2.40    End= 172.16.2.46
                     Port Start= 0              End=N/A
        Enable Replay Detection = No
        Key Management= IKE
        Edit IKE Setup= No
        Edit Manual Setup= N/A



                Press ENTER to Confirm or ESC to Cancel:
```

Figure 23-7 Menu 27.1.1 — IPSec Setup

Table 23-4 Menu 27.1.1 — IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Index	This is the VPN rule index number you selected in the previous menu.	**1**
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed **Menu 27.1 - IPSec Summary**.	
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.	**Yes**
My IP Addr	This is the IP address of your ZyWALL. If this field is left as 0.0.0.0, then the ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) in setting up the VPN tunnel. If this IP address changes after setup, the VPN tunnel will have to be rebuilt.	0.0.0.0
Secure Gateway IP Addr	This is the WAN IP address of the IPSec router with which you're making the VPN connection. If the peer has a dynamic WAN IP address, set this field to 0.0.0.0. This may be useful for telecommuters initiating a VPN	Real IP address

Table 23-4 Menu 27.1.1 — IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
Secure Gateway IP Addr	This is the WAN IP address of the IPSec router with which you're making the VPN connection. If the peer has a dynamic WAN IP address, set this field to 0.0.0.0. This may be useful for telecommuters initiating a VPN tunnel to the company network. Only the telecommuter may initiate the VPN tunnel in this case.	Real IP address
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.	0
Local	Local IP addresses must be static and correspond to the peer's configured remote IP address range.	
IP Addr Start	Enter the beginning IP address of the computers on your local network behind your ZyWALL. This must be a fixed IP address.	192.168.1.35
End	Enter the end IP address of the computers on your local network behind your ZyWALL.	192.168.1.38
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3	0
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field.	
Remote	Remote IP addresses must be static and correspond to the initiator's configured local IP address range.	
IP Addr Start	Enter the beginning IP address of the computers on the remote network behind the remote IPSec router. This must be a fixed IP address.	172.16.2.40
End	Enter the end IP address of the computers on the remote network behind the remote IPSec router.	172.16.2.46
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3	0
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field.	
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**.	**No**

Table 23-4 Menu 27.1.1 — IPSec Setup

FIELD	DESCRIPTION	EXAMPLE
	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.	
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. If you choose **IKE**, then you must configure the IKE Setup menu. Move the cursor to the **Edit IKE Setup** field, press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to the IKE Setup menu. If you choose **Manual**, then you must configure the **ESP**/**AH** Setup menu. Move the cursor to the **Edit Manual Setup** field, press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to the IKE Setup menu. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.	**IKE**
Edit IKE Setup	You must configure this menu when you choose **IKE** key management. Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to **Menu 27.1.1.1 – IKE Setup** discussed next.	**No**
Edit Manual Setup	You must configure this menu when you choose **Manual** key management. Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to display **Menu 27.1.1.2 – Manual Setup** discussed later.	**N/A**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

23.4 IKE Setup

To edit this menu, move the cursor to the **Edit IKE Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

23.4.1 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

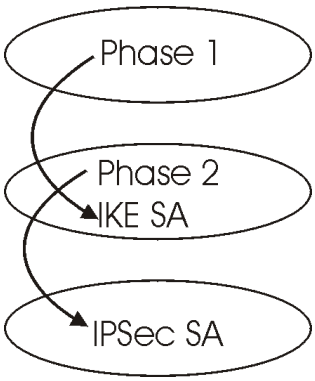


Figure 23-8 Two Phases to set up the IPSec SA

In phase 1 you must:

- Choose a negotiation mode
- Authenticate the connection by entering a pre-shared key
- Choose an encryption algorithm
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long IKE SA negotiation should proceed before it times out. A value of **0** means IKE SA negotiation never times out. If IKE SA negotiation times out, then both IKE SA and IPSec SA must be renegotiated.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange
- Choose an encryption algorithm
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section 23.4.5*. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode
- Set the IPSec SA lifetime. This field allows you to determine how long IPSec SA setup should proceed before it times out. A value of **0** means IPSec SA never times out. If IPSec SA negotiation times out, then the IPSec SA must be renegotiated (but not the IKE SA).

23.4.2 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips (SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number)). This mode features identity protection (your identity is not revealed in the negotiation).

- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

23.4.3 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

23.4.4 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

23.4.5 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.
This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyWALL. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

```
                    Menu 27.1.1.1 - IKE Setup

          Phase 1
            Negotiation Mode= Main
            Pre-Shared Key=
            Encryption Algorithm = DES
            Authentication Algorithm = SHA1
            SA Life Time (Seconds)= 0
            Key Group= DH1

          Phase 2
            Active Protocol  = ESP
            Encryption Algorithm  = DES
            Authentication Algorithm  = SHA1
            SA Life Time (Seconds)[0: unspecified]= 0
            Encapsulation  = Tunnel
            Perfect Forward Secrecy (PFS)= None


                    Press ENTER to Confirm or ESC to Cancel:
```

Figure 23-9 Menu 27.1.1.1 — IKE Setup

Table 23-5 Menu 27.1.1.1 — IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Phase 1		
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes.	**Main**
Pre-Shared Key	ZyWALL gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated.	
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. ZyWALL **DES** encryption algorithm uses a 56-bit key. Strong Encryption, or Triple DES (**3DES**), is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in slightly increased latency and decreased throughput. Press [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER].	**DES**
Authentication	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash	**SHA1**

Table 23-5 Menu 27.1.1.1 — IKE Setup

FIELD	DESCRIPTION	EXAMPLE
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slightly slower. Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**SHA1**
SA Life Time (Seconds)]	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 300 to 86,400 seconds (one day). A short **SA Life Time** increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. A value of **0** means IKE SA negotiation never times out.	**0**
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.	**DH1**
Phase 2		
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.	**ESP**
Encryption Algorithm	Press [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER].	**DES**
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].	**MD5**
SA Life Time (Seconds)[0: unspecified]	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 300 to 86,400 seconds (one day). A value of **0** means IPSec SA never times out.	**0**
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.	**Tunnel**
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).	**None**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

23.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

23.5.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. These parameters have been discussed earlier.

Table 23-6 Active Protocol — Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

23.5.2 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPSec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

```
                Menu 27.1.1.2 - Manual Setup
Active Protocol= ESP Tunnel

ESP Setup
  SPI=
  Encryption Algorithm= DES
    Key1=
    Key2=
    Key3=
  Authentication Algorithm= MD5
    Key= N/A

AH Setup
  SPI (Decimal)= N/A
  Authentication Algorithm= N/A
    Key=

      Press ENTER to Confirm or ESC to Cancel:
```

Figure 23-10 Menu 27.1.1.2 — Manual Setup

Table 23-7 Menu 27.1.1.2 — Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)	**ESP Tunnel**
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.	
SPI	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.	1234
Encryption Algorithm	Press [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.	**DES**
Key1	The key must be unique and eight characters long. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.	89abcde
Key2	The key must be unique, eight characters long and can be comprised of any character including spaces (but trailing spaces are truncated).	
Key3	The key must be unique, eight characters long and can be comprised of any character including spaces (but trailing spaces are truncated).	
Authentication	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press	**MD5**

Table 23-7 Menu 27.1.1.2 — Manual Setup

FIELD	DESCRIPTION	EXAMPLE
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**MD5**
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	123456789abcde
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.	
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.	**N/A**
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].	**N/A**
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.	**N/A**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 24
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

1.1. Introduction

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

An SA times out automatically after one minute if there is no traffic.

1. Use the **Refresh** function to display active VPN connections.
2. Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

```
                        Menu 27.2 - SA Monitor

 #                  Name                    Encap.     IPSec Algorithm
---   --------------------------------   ---------   ----------------
001    Taiwan : 3.3.3.1 - 3.3.3.3.100      Tunnel     ESP DES MD5
002
003
004
005
006
007
008
009
010
                  Select Command= Refresh
                  Select Connection= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figure 24-1 Menu 27.2 — SA Monitor

Table 24-1 Menu 27.2 — SA Monitor

FIELD	DESCRIPTION	EXAMPLE
#	This is the security association index number.	
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a	**Taiwan**

Table 24-1 Menu 27.2 — SA Monitor

FIELD	DESCRIPTION	EXAMPLE
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address. When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this the same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.	**Taiwan**
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.	**Tunnel**
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**.An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits). Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).	**ESP DES MD5**
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect**, **None**, **Next Page**, or **Previous Page** and then press [ENTER]. You must select a connection in the next field when you choose the **Disconnect** command. **Refresh** displays current active VPN connections. **None** allows you to jump to the “Press ENTER to Confirm…” prompt. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).	**Refresh**
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].	**1**
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

Chapter 25
IPSec Log

This chapter interprets common IPSec log messages.

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log as shown next. The following figure shows a typical log from the initiator of a VPN connection.

```
Index:    Date/Time:              Log:
-----------------------------------------------------------
 001    01 Jan 08:02:22    !! Cannot find outbound SA for rule <1>
 002    01 Jan 08:02:22    Send Main Mode request to <192.168.100.101>
 003    01 Jan 08:02:22    Send:<SA>
 004    01 Jan 08:02:22    Recv:<SA>
 005    01 Jan 08:02:24    Send:<KE><NONCE>
 006    01 Jan 08:02:24    Recv:<KE><NONCE>
 007    01 Jan 08:02:26    Send:<ID><HASH>
 008    01 Jan 08:02:26    Recv:<ID><HASH>
 009    01 Jan 08:02:26    Phase 1 IKE SA process done
 010    01 Jan 08:02:26    Start Phase 2: Quick Mode
 011    01 Jan 08:02:26    Send:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:02:26    Recv:<HASH><SA><NONCE><ID><ID>
 013    01 Jan 08:02:26    Send:<HASH>
 Clear IPSec Log (y/n):
```

Figure 25-1 Example VPN Initiator IPSec Log

The following figure shows a typical log from the VPN connection peer.

```
Index:    Date/Time:              Log:
-----------------------------------------------------------
 001    01 Jan 08:08:07    Recv Main Mode request from <192.168.100.100>
 002    01 Jan 08:08:07    Recv:<SA>
 003    01 Jan 08:08:08    Send:<SA>
 004    01 Jan 08:08:08    Recv:<KE><NONCE>
 005    01 Jan 08:08:10    Send:<KE><NONCE>
 006    01 Jan 08:08:10    Recv:<ID><HASH>
 007    01 Jan 08:08:10    Send:<ID><HASH>
 008    01 Jan 08:08:10    Phase 1 IKE SA process done
 009    01 Jan 08:08:10    Recv:<HASH><SA><NONCE><ID><ID>
 010    01 Jan 08:08:10    Start Phase 2: Quick Mode
 011    01 Jan 08:08:10    Send:<HASH><SA><NONCE><ID><ID>
 012    01 Jan 08:08:10    Recv:<HASH>
 Clear IPSec Log (y/n):
```

Figure 25-2 Example VPN Responder IPSec Log

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

Double exclamation marks (!!) denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

Table 25-1 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
`Cannot find outbound SA for rule <#d>`	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
`Send Main Mode request to <IP>` `Send Aggressive Mode request to <IP>`	The ZyWALL has started negotiation with the peer.
`Recv Main Mode request from <IP>` `Recv Aggressive Mode request from <IP>`	The ZyWALL has received an IKE negotiation request from the peer.
`Send:<Symbol><Symbol>` `Recv:<Symbol><Symbol>`	IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log - see *Table 25-3*.
`Phase 1 IKE SA process done`	Phase 1 negotiation is finished.
`Start Phase 2: Quick Mode`	Phase 2 negotiation is beginning using Quick Mode.
`!! IKE Negotiation is in process`	The ZyWALL has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.
`!! Duplicate requests with the same cookie`	The ZyWALL has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.
`!! No proposal chosen`	The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.
`!! Verifying Local ID failed` `!! Verifying Remote ID failed`	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.

Table 25-1 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
!! Local / remote IPs of incoming request conflict with rule <#d>	If the security gateway is "0.0.0.0", the ZyWALL will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.
!! Invalid IP <IP start>/<IP end>	The peer's "Local IP Addr" range is invalid.
!! Remote IP <IP start> / <IP end> conflicts	If the security gateway is "0.0.0.0", the ZyWALL will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the ZyWALL will not accept VPN connection requests from this peer.
!! Active connection allowed exceeded	The ZyWALL limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
!! IKE Packet Retransmit	The ZyWALL did not receive a response from the peer and so retransmits the last packet sent.
!! Failed to send IKE Packet	The ZyWALL cannot send IKE packets due to a network error.
!! Too many errors! Deleting SA	The ZyWALL deletes an SA when too many errors occur.

The following table shows sample log messages during packet transmission.

Table 25-2 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the ZyWALL's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0".. If this field is configured as 0.0.0.0, then the ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find Phase 2 SA	The ZyWALL cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Discard REPLAY packet	If the ZyWALL receives a packet with the wrong sequence number it will discard it.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Please check them.

Table 25-2 Sample IPSec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
`!! Inbound packet decryption failed`	The decryption configuration settings are incorrect. Please check them.
`Rule <#d> idle time out, disconnect`	If an SA has no packets transmitted for a period of time (configurable via CI command), the ZyWALL drops the connection.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 25-3 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Part VI:

Troubleshooting, Appendices and Index

This part provides Troubleshooting, followed by some Appendices and an Index.

Chapter 26
Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. Please see our included disk for further information.

26.1 Problems Starting Up the ZyWALL

Table 26-1 Troubleshooting the Start-Up of your ZyWALL

PROBLEM	CORRECTIVE ACTION	
None of the LEDs are on when you turn on the ZyWALL.	Check the connection between the power adapter and the ZyWALL. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
Cannot access the ZyWALL via the console port.	1. Check to see if the ZyWALL is connected to your computer's serial port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 data bits, 1 stop bit, data flow set to none.

26.2 Problems with the LAN Interface

Table 26-2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Can't ping any workstation on the LAN.	Check the 10M/100M LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
	Verify that the IP address and the subnet mask are consistent between the ZyWALL and the workstations.

26.3 Problems with the WAN interface

Table 26-3 Troubleshooting the WAN interface

PROBLEM	CORRECTIVE ACTION
Cannot get WAN IP from the ISP.	The WAN IP is provided when the ISP recognizes the user as an authorized user after verifying the MAC address or Host Name or User ID. Find out the verification method used by your ISP.
	If the ISP checks the LAN MAC Address, tell the ISP the WAN MAC address of the ZyWALL. The WAN MAC can be obtained from menu 24.1. In case the ISP does not allow you to use a new MAC, you can clone the MAC from the LAN as the WAN MAC and send it to the ISP using **Menu 2 - WAN Setup**. We recommend you configure this menu anyway even if your ISP presently does not require MAC address authentication
	If the ISP checks the Host Name, enter host name in the **System Name** field in **Menu 1 - General Setup** when you connect the ZyWALL to a cable/xDSL modem.
	If the ISP checks the User ID, make sure that you have entered the correct **Service Type**, user name (in the **My Login** field) and password (in the **My Password** field) in **Menu 4 - Internet Access Setup**.

Table 26-3 Troubleshooting the WAN interface

PROBLEM	CORRECTIVE ACTION
Can't connect to a remote node or ISP.	Check menu 24.1 to verify the line status. If it indicates **Down**, then refer to the section on the line problems.

26.4 Problems with Internet Access

Table 26-4 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
Cannot access the Internet.	Connect your cable / xDSL modem with the ZyWALL using appropriate cable. Check with the manufacturer of your cable / xDSL device about your cable requirement because for some devices may require crossover cable and others a regular straight-through cable.
	Verify your settings in menu 3.2 and menu 4.

26.5 Problems with the Password

Table 26-5 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL.	The **Password** field is case sensitive. Make sure that you enter the correct password using the proper casing.
	If you forget your password you will need to restore the factory default configuration file. This will restore all of the factory defaults including the password. See *the Resetting the ZyWALL* section for details.

26.6 Problems with Remote Management

Table 26-6 Troubleshooting Remote Management

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN or WAN.	Refer to the *Remote Management Limitations* section for scenarios when remote management may not be possible.
	When NAT is enabled: ➢ Use the ZyWALL's WAN IP address when configuring from the WAN. ➢ Use the ZyWALL's LAN IP address when configuring from the LAN.
	Refer to the *Problems with the LAN Interface* section for instructions on checking your LAN connection.
	Refer to the *Problems with the WAN Interface* section for instructions on checking your WAN connection

Appendix A
The Big Picture

The following figure gives an overview of how filtering, the firewall, VPN and NAT are related.

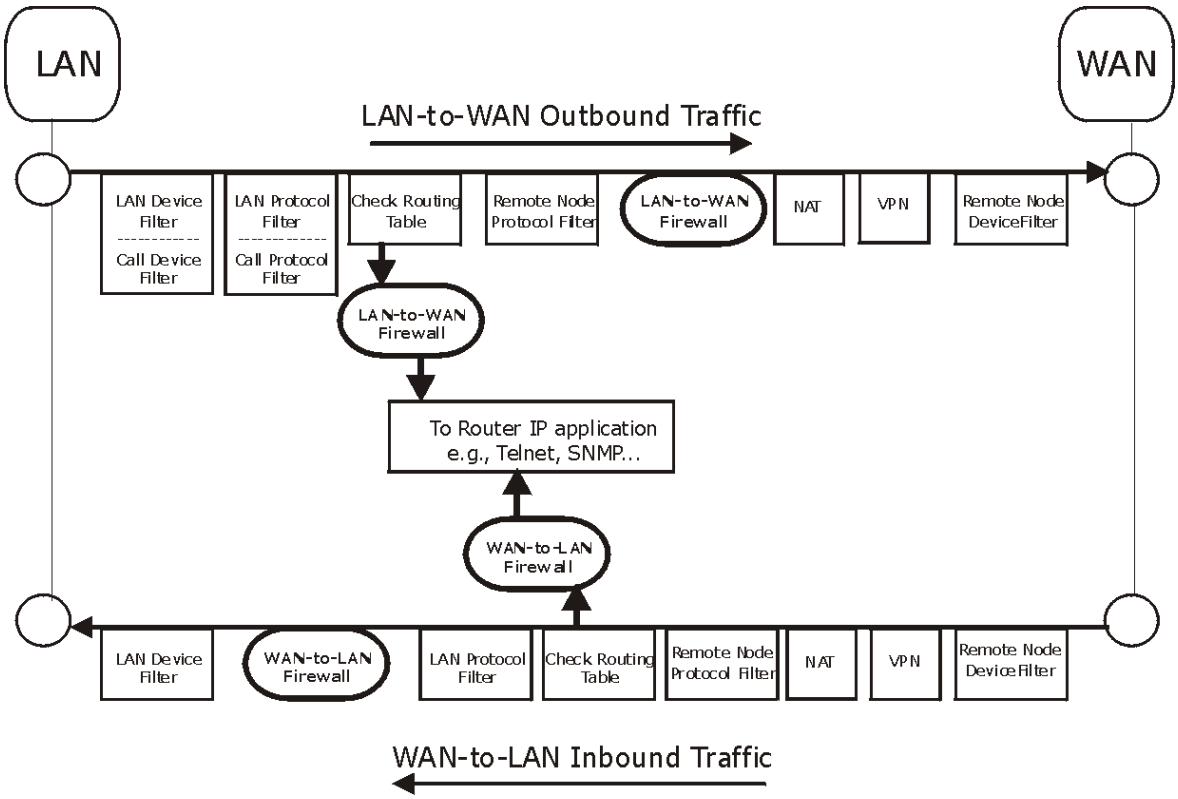


Diagram 1 Big Picture — Filtering, Firewall, NAT and VPN

Appendix B
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) that connects to a xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

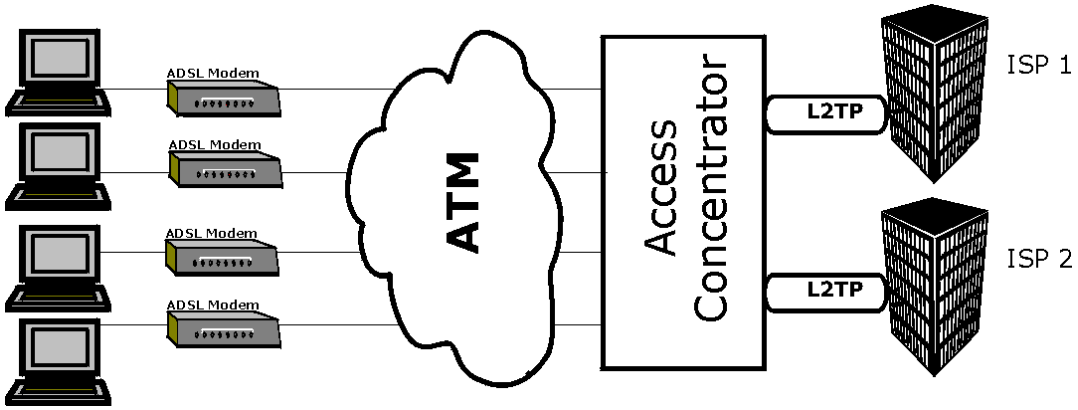


Diagram 2 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

ZyWALL as a PPPoE Client

When using the ZyWALL as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

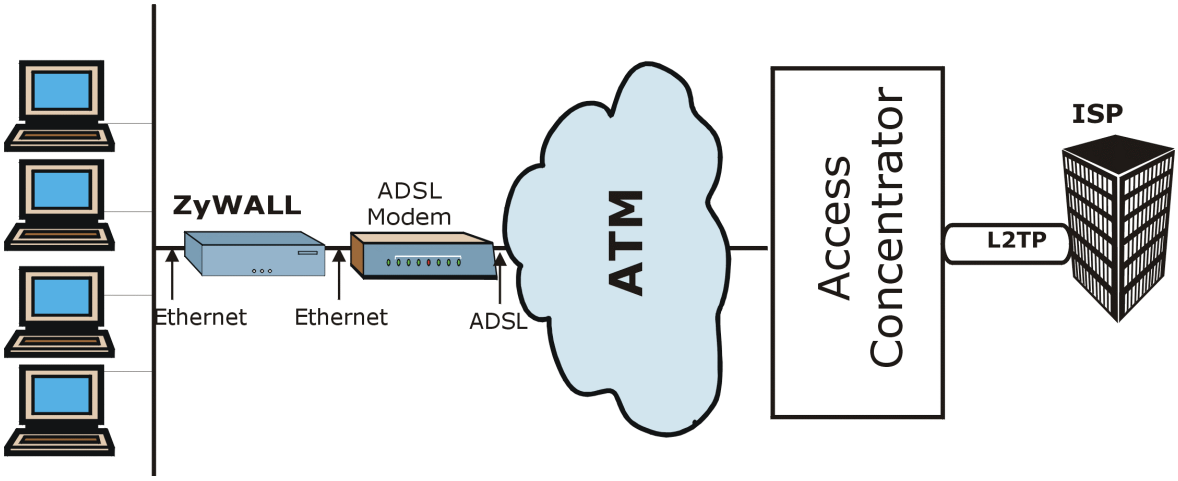


Diagram 3 ZyWALL as a PPPoE Client

Appendix C
PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

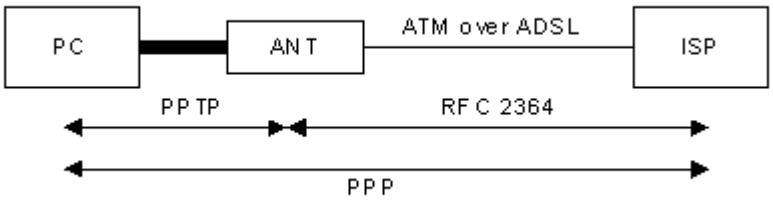


Diagram 4 Transport PPP frames over Ethernet

PPTP and the ZyWALL

When the ZyWALL is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyWALL's Internet connection. In NAT mode, the ZyWALL is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The ZyWALL initializes the PPTP connection hence, there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

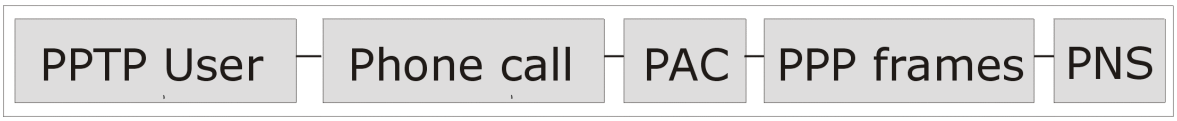


Diagram 5 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the ZyWALL, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

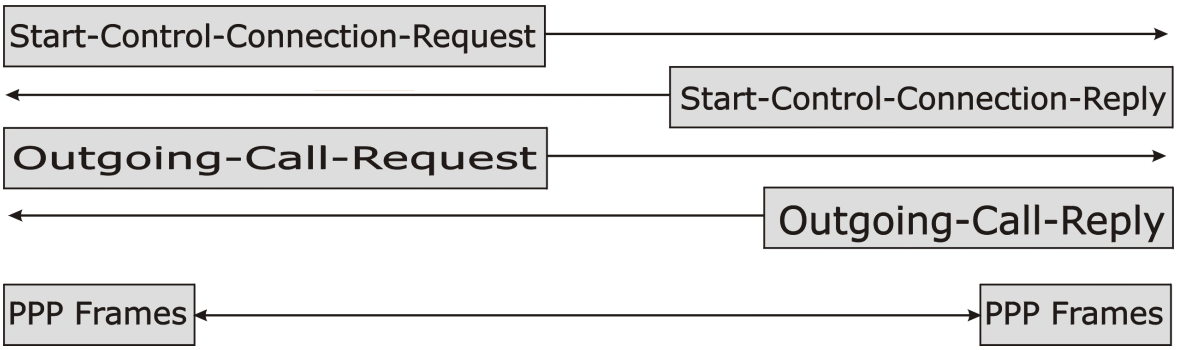


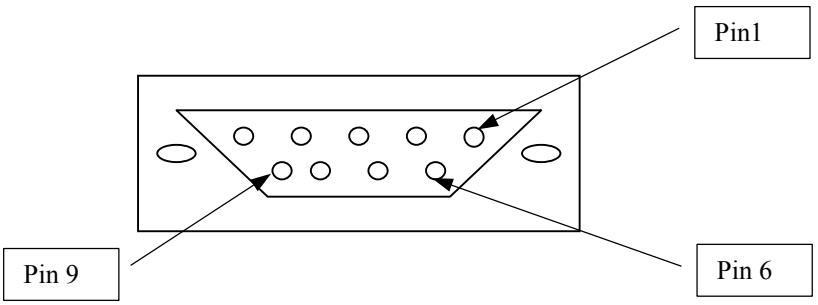
Diagram 6 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix D
Hardware Specifications

Power Specification	I/P AC 120V / 60Hz ; O/P DC 12V 1200 mA
MTBF	100000 hrs
Operation Temperature	0º C ~ 40º C
Ethernet Specification for WAN	10Mbit Half Duplex
Ethernet Specification for LAN	10/100 Mbit Half / Full Auto-negotiation
Console Port RS – 232	Pin 1 = NON ; Pin 2 = DTE-RXD; Pin 3 = DTE-TXD; Pin 4 = DTE-DTR; Pin 5 = GND; Pin 6 = DTE-DSR; Pin 7 = DTE-RTS; Pin 8 = DTE-CTS; PIN 9 = NON. See Figure below



WAN/LAN Cable Pin Layout: Straight-Through			Crossover		
(Switch)		(Adapter)	(Switch)		(Switch)
1 IRD +	———	1 OTD +	1 IRD +	———	1 IRD +
2 IRD -	———	2 OTD -	2 IRD -	———	2 IRD -
3 OTD +	———	3 IRD +	3 OTD +	———	3 OTD +
6 OTD -	———	6 IRD -	6 OTD -	———	6 OTD -

Appendix E
Important Safety Instructions

The following safety instructions apply to the ZyWALL.

1. Be sure to read and follow all warning notices and instructions.
2. The maximum recommended ambient temperature for the ZyWALL is 40º Celsius (104º Fahrenheit).Care must be taken to allow sufficient air circulation or space between units when the ZyWALL is installed inside a closed rack assembly. The operating ambient temperature of the rack environment might be greater than room temperature.
3. Installation in a rack without sufficient airflow can be unsafe.
4. Racks should safely support the combined weight of all equipment.
5. The connections and equipment that supply power to the ZyWALL should be capable of operating safely with the maximum power requirements of the ZyWALL. In case of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the ZyWALL is printed on the nameplate.
6. The AC adapter must plug in to the right supply voltage, i.e. 120VAC adapter for North America and 230VAC adapter for Europe. Make sure that the supplied AC voltage is correct and stable. If the input AC voltage is over 10% lower than the standard may cause the ZyWALL to malfunction.
7. Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
8. Do not allow anything to rest on the power cord of the AC adapter, and do not locate the product where anyone can walk on the power cord.
9. Do not service the product by yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
10. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
11. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products. If the equipment is to be used with telecommunications circuit, take the following precautions:
    - Never install telephone wiring during a lightning storm.

- Never install telephone jacks in wet location unless the jack is specially designed for wet location.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.

Appendix F
Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main system firmware (ZyNOS) is started. When you start up your ZyWALL, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the *Firmware and Configuration File Maintenance* chapter.

```
Bootbase Version: V2.02 | 10/11/2000 13:58:03
RAM: Size = 8192 Kbytes
DRAM Post: Testing:  8192K OK
FLASH: Intel 16M

ZyNOS Version: V324\wa0b05 | 3/5/2001 18:00:34

Press any key to enter debug mode within 3 seconds.
```

Diagram 7 Option to Enter Debug Mode

Enter ATHE to view all available ZyWALL boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

```
                    ======= Debug Command Listing =======
AT              just answer OK
ATHE            print help
ATBAx           change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)       set BootExtension Debug Flag (y=password)
ATSE            show the seed of password generator
ATTI(h,m,s)     change system time to hour:min:sec or show current time
ATDA(y,m,d)     change system date to year/month/day or show current date
ATDS            dump RAS stack
ATDT            dump Boot Module Common Area
ATDUx,y         dump memory contents from address x for length y
ATRBx           display the  8-bit value of address x
ATRWx           display the 16-bit value of address x
ATRLx           display the 32-bit value of address x
ATGO(x)         run program at addr x or boot router
ATGR            boot router
ATGT            run Hardware Test Program
ATRTw,x,y(,z)   RAM test level w, from address x to y (z iterations)
ATSH            dump manufacturer related data in ROM
ATDOx,y         download from address x for length y to PC via XMODEM
ATTD            download router configuration to PC via XMODEM
ATUR            upload router firmware to flash ROM
ATLC            upload router configuration file to flash ROM
ATXSx           xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSR            system reboot
```

Diagram 8 Boot Module Commands

Appendix G
Firewall CLI Commands

The following table describes the syntax used to configure your firewall using Command Line Interface (CLI) commands. Select **Menu 24.8 - Command Interpreter Mode** from the main menu to go into CLI mode. For details on other CLI commands to configure your ZyWALL, please consult the included disk.

FUNCTION	CLI SYNTAX	DESCRIPTION
Firewall Set-Up		
	`config edit firewall active <yes | no>`	Activates or deactivates the saved firewall settings.
	`config retrieve firewall`	Retrieves currently saved firewall settings.
	`config save firewall`	Saves the current firewall settings.
Display		
	`config display firewall`	Displays the all the firewall settings including e-mail, attack, and sets/rules.
	`config display firewall set <set #>`	Displays current entries of a set configuration; including timeout values, name, default-permit, and number of rules under it. If you don't put # after set, it will display all the sets/rules information.
	`config display firewall set <set #> rule <rule #>`	Displays current entries of a rule in a set configuration;
	`config display firewall attack`	Displays all the settings for attack alert.
	`config display firewall e-mail`	Displays all the setting for e-mail part.
	`config display firewall ?`	Displays all the available sub commands.
Edit		
E-mail	`config edit firewall e-mail mail-server <ip address of mail server>`	Edits the mail server which alerting e-mail messages are sent through.
	`config edit firewall e-mail return-addr <e-mail address>`	Edits the source address for sending mail usage.

FUNCTION	CLI SYNTAX	DESCRIPTION
	config edit firewall e-mail email-to <e-mail address>	Edits the mail address which you want to send the alert to.
	config edit firewall e-mail policy <full | hourly | daily | weekly>	Edits whether the current firewall traffic log contents are sent through e-mail when the log is full, hourly, daily, or weekly.
	config edit firewall e-mail day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>	Edits the day the current firewall traffic log contents are sent through e-mail; pertains to the weekly policy.
	config edit firewall e-mail hour <0-23>	Edits the hour of the day the current firewall traffic log contents are sent through e-mail; pertains to the hourly, daily & weekly policies.
	config edit firewall e-mail minute <0-59>	Edits the minute of the hour the current firewall traffic log contents are sent through e-mail; pertains to the hourly, daily & weekly policies.
Attack	config edit firewall attack send-alert <yes | no>	Activates or deactivates the firewall DOS attack notification e-mails.
	config edit firewall attack block <yes | no>	Yes: to block the traffics when exceeds the threshold of tcp-max-incomplete . No: to delete the oldest half-open session when exceeds the threshold of tcp-max-incomplete.
	config edit firewall attack block-minute <0-255>	Only valid when sets block to be yes. The unit is minute.
	config edit firewall attack minute-high <0-255>	The threshold to start to delete the old half-opened sessions to minute-low.
	config edit firewall attack minute-low <0-255>	The threshold to stop the deletion of the half-opened sessions.
	config edit firewall attack max-incomplete-high <0-255>	The threshold to start to delete the old half-opened sessions to max-incomplete-low.
	config edit firewall attack max-incomplete-low <0-255>	The threshold to stop the deletion of the half-opened sessions.

FUNCTION	CLI SYNTAX	DESCRIPTION
	config edit firewall attack tcp-max-incomplete <0-255>	The threshold to start executing the block field.
Sets	config edit firewall set <set #> name <desired name>	Edits the name for a specified set.
	Config edit firewall set <set #> default-permit <forward | block>	Edits whether a packet is dropped or allowed through, when it does not meet a rule within the set.
	Config edit firewall set <set #> icmp-timeout <seconds>	Edits the time limit, in seconds, for an idle ICMP session, before it is terminated.
	Config edit firewall set <set #> udp-idle-timeout <seconds>	Edits the time limit, in seconds, for an idle UDP session, before it is terminated.
	Config edit firewall set <set #> connection-timeout <seconds>	Edits the wait time, in seconds, for the SYN traffic in initiating a TCP session, before it is terminated.
	Config edit firewall set <set #> fin-wait-timeout <seconds>	Edits the wait time, in seconds, for the FIN traffic in concluding a TCP session, before it is terminated.
	Config edit firewall set <set #> tcp-idle-timeout <seconds>	Edits the time limit, in seconds, for an idle TCP session, before it is terminated.
	Config edit firewall set <set #> log <yes | no>	Switches on/off the logs for matching default permit.
Rules	Config edit firewall set <set #> rule <rule #> permit <forward | block>	Edits whether a packet is dropped or allowed through, when it meets this rule.
	Config edit firewall set <set #> rule <rule #> active <yes | no>	Edits whether a rule is enabled or not.
	Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >	Edits the protocol specification number made in this rule for ICMP currently.
	Config edit firewall set <set #> rule <rule #> log <none | match | not-match | both>	Edits whether traffic that does match the rule, doesn't match, both or neither is logged.
	Config edit firewall set <set #>	Activates or deactivates the notification function, for when a

FUNCTION	CLI SYNTAX	DESCRIPTION
	rule <rule #> alert <yes | no>	DOS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an e-mail to the SMTP destination address and log an alert.
	config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>	Selects and edits a source address of the traffic which comply to this rule.
	config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>	Selects and edits a source address and subnet mask of traffic which comply to this rule.
	config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>	Selects and edits a source address range of traffic which comply to this rule.
	config edit firewall set <set #> rule <rule #> destaddr-single <ip address>	Selects and edits a destination address of the traffic which comply to this rule.
	config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask>	Selects and edits a destination address and subnet mask of traffic which comply to this rule.
	config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address>	Selects and edits a destination address range of traffic which comply to this rule.
	config edit firewall set <set #> rule <rule #> TCP destport-single <port #>	Selects and edits the destination port of the traffic which comply with this rule. For non-consecutive port numbers, the user may repeat this command line to enter in the multiple port numbers.
	config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #>	Selects and edits a destination port range of traffic which comply to this rule.

FUNCTION	CLI SYNTAX	DESCRIPTION
	config edit firewall set <set #> rule <rule #> UDP destport-single <port #>	Selects and edits the destination port of the traffic which comply with this rule. For non-consecutive port numbers, the user may repeat this command line to enter in the multiple port numbers.
	config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #>	Selects and edits a destination port range of traffic which comply to this rule.
	config edit firewall set<set #> rule <rule #> destport-custom <desired custom port name>	Types in the desired custom port name.
Delete		
	config delete firewall e-mail	Removes all the settings for e-mail alert.
	config delete firewall attack	Resets all the settings for attack to default setting.
	config delete firewall set <set #>	Removes the specified set from the firewall configuration.
	config delete firewall set <set #> rule <rule #>	Removes the specified rule in a set from the firewall configuration.

Appendix H
Power Adapter Specifications

AC Power Adapter Specifications
North America
AC Power Adapter model AD48-1201200DUY
Input power: AC120Volts/60Hz/0.25A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: North American standards
Safety standards: UL, CUL (UL 1950, CSA C22.2 No.234-M90)
AC Power Adapter model AD48-1201200DUY
Input power: AC120Volts/60Hz
Output power: DC12Volts/1.2A
Power consumption: 9 W
Plug: North American standards
Safety standards: UL, CUL (UL1950, CSA C22.2 NO. 234-M90)
European Union
AC Power Adapter model AD-1201200DV
Input power: AC230Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)
AC Power Adapter model JAD-121200E
Input power: AC230Volts/50Hz,
Output power: DC12Volts/1.2A
Power consumption: 9 W

Plug: European Union standards
Safety standards: TUV, CE (EN 60950)

UK
AC Power Adapter model AD-1201200DK
Input power: AC230Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: United Kingdom standards
Safety standards: TUV, CE (EN 60950, BS7002)

Japan
AC Power Adapter model JOD-48-1124
Input power: AC100Volts/ 50/60Hz/ 27VA
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Japan standards
Safety standards: T-Mark

Australia and New Zealand
AC Power Adapter model AD-1201200Ds or AD-121200DS
Input power: AC240Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Australia and New Zealand standards
Safety standards: NATA (AS 3260)

Index

A

Action for Matched Packets 10-11
Activate The Firewall..... 13-3
Alert Schedule..... 9-5
Application-level Firewalls..... 7-1
Applications for the ZyWALL 10..... 1-4
AT command..... 18-2
Attack
  Reasons..... 12-2
Attack Alert..... 9-7, 9-9
Attack Types 7-6
  Reason 8-3
Authentication 4-4, 4-5
auto-negotiation 1-1

B

backup 18-2
Blocking Time 9-8, 9-9, 9-11
Boot Commands ..... K
Broadband Access Security Gateway .... i, xxxi, 1-1
Brute-force Attack, ... 7-6
Budget Management..... 19-2, 19-3

C

Cable Modem..... 2-3, 2-4, 7-2
Call Control 19-2
Call History..... 19-4
Call Scheduling 21-1
  maximum number of schedule sets 21-1
  PPPoE 21-3
  precedence 21-1
  precedence example..... *See* precedence
Call-Trigerring Packet 17-10
CDR 17-7
certification..... v
CHAP 4-5
CLI Commands ..... M
Command Interpreter Mode..... 19-1
Conditions that prevent TFTP and FTP from
  working over WAN 18-4
Configuring A POP Custom Port 13-8
Console Port..... 2-3, 17-3, 17-4, 17-5, H
Content Filtering 14-1
  Categories 14-1
  Customizing..... 14-2
  Days and Times..... 14-1
  Exempt Computers..... 14-1
  Filter List..... 14-1
  Keywords..... 14-2
  Log Records 14-2
  Restrict Web Features..... 14-1
  Update List 14-1
Copyright ii
Custom Ports
  Creating/Editing 11-3
  Introduction..... 11-1
Customer Support vii
Customized Services..... 11-2

D

Default Policy Log..... 10-6
Denial of Service 7-2, 7-3, 8-1, 9-8
Denial of Services
  Thresholds..... 9-10
DestAdd..... 13-11
Destination Address..... 10-3, 10-10
DHCP (Dynamic Host Configuration Protocol) 1-3,
  5-2
DHCP Ethernet Setup..... 5-5
DHCP Negotaition and Syslog Connection from
  the Internet – EG 3 13-12
DHCP Negotiation 13-12
Diagnostic..... 17-11
DNS 5-2
Domain Name..... 5-2, 6-13, 17-3
DoS
  Basics 7-3

Types 7-4
DoS (Denial of Service) 1-1
Dynamic DNS 4-1

E

E-mail
Log Example 9-6
Mail Server 9-5
Mail Subject 9-5
Tab 9-4
E-mail Alerts 9-5
E-mail Screen 13-4
Encapsulation
PPP over Ethernet C
Ethernet Encapsulation ... 6-1, 4-1, 4-2, 4-6, 4-7, 4-11, 6-13
Examples 13-1

F

Factory Default 4-4
Factory LAN Defaults 5-2
Features of The ZyWALL 10 1-1
Filename Conventions 18-1
Filter 5-1, 4-11, 15-1
About 15-1
Applying 15-18
Configuring 15-4
Example 15-14
Filter log 17-8
Generic Filter Rule 15-12
NAT 15-17
Structure 15-2
Filters
Executing a Filter Rule 15-2
Logic Flow of an IP Filter 15-10
Firewall
Access Methods 8-1
Activating 8-1
Address Type 10-13
Alerts 9-3
Connection Direction 10-3
Creating/Editing Rules 10-10
Custom Ports ..... *See* Custom Ports
E-mail 9-3
Enabling 9-3
Firewall Vs Filters 7-12
Guidelines For Enhancing Security 7-11
Introduction 7-2
LAN to WAN Rules 10-3
Log 8-2
Log Timer 9-5
Logs 9-4
Policies 10-1
Remote Management 8-1
Rule Checklist 10-1
Rule Examples 13-1
Rule Logic 10-1
Rule Precedence 10-4
Rule Security Ramifications 10-2
Rule To Allow Web Service From The Internet 13-1
Services 10-7
SMT Menus 8-1
Types 7-1
When To Use 7-13
Flow Control 2-5
Front Panel LEDs 2-1
FTP 20-3
FTP File Transfer 18-11
FTP Restrictions 18-4, 20-3
FTP Server 1-3, 6-19

G

General Setup 4-1
Getting Started I

H

Half-Open Sessions 9-8
Hidden Menus 3-2
HTML Help ..... *See*
HTTP 6-14, 7-1, 7-3, 7-4, 23-9
HyperTerminal program 18-6, 18-9

I

IANA 5-3
ICMP echo 7-6
idle timeout 4-4

IGMP (Internet Group Multicast Protocol) 5-4
Initial Screen 3-1
Installation Requirements 2-5
Internet Access Setup 6-1, 6-6, 26-2
Internet Access via Cable or xDSL Modem 1-4
Internet Assigned Numbers Authority .... *See* IANA
Internet Control Message Protocol (ICMP) 7-6
IP address 5-3, 5-7
IP Address Assignment 4-7, 4-9
IP Alias 1-2, 5-5
IP Alias Setup 5-7
IP Multicast 1-2, 5-4
IP Network Number 5-3
IP Pool 5-2, 5-6
IP Ports 7-4, 23-9
IP Spoofing 7-4, 7-7
IP Static Route 5-1, 5-2, 5-3
IPSec standard 1-1
IPSec VPN Capability 1-1

K

Key Fields For Configuring Rules 10-2

L

LAN Setup 5-1, 5-5
LAN to WAN Rules 10-3
LAND 7-4, 7-6
Local Network
Rule Summary 10-4
log 17-5
Log Facility 17-7
Log Screen 12-1
Logs 12-1

M

MAC Address 4-4, 26-2
Mail Server 9-5
Main Menu 3-3
Management Information Base (MIB) 16-2
Maximum Incomplete High 9-10
Maximum Incomplete Low 9-10
Max-incomplete High 9-8
Max-incomplete Low 9-8, 9-10
Metric 4-7, 4-9, 5-3
My WAN Address 4-9

N

nailed-up connection *4-4*
NAT 4-7, 4-9, 15-17
Application 6-3
Applying NAT in the SMT Menus 6-6
Configuring 6-8
Definitions 6-1
Examples 6-16
How NAT Works 6-2
Mapping Types 6-4
Non NAT Friendly Application Programs 6-22
Ordering Rules 6-11
What NAT does 6-2
NetBIOS commands 7-6
Network Address Translation (NAT) 1-3, 6-1

O

One Minute High 9-10
One Minute Low 9-10
One-Minute High 9-8
Online Registration vi

P

Packet Filtering 7-13
Packet Filtering Firewalls 7-1
Packet Information 12-2
Packet Triggered 17-7
Packing List Card xxxii
PAP 4-5
Password 3-1, 3-7
Ping 17-13
Ping of Death 7-4
POP3 ..... 7-3, 7-4
Port Configuration 11-4
Power Adapter 2-4
PPP log 17-8
PPPoE Encapsulation .. 6-1, 6-4, 4-1, 4-3, 4-4, 4-5, 4-10, 4-11
PPTP Client 6-3

PPTP Encapsulation.....1-2, 6-2, 4-5, 4-8
Private 5-3, 5-4, 4-8, 4-10, 5-3
Private IP Addresses 5-3

R

Read Me First xxxi
Rear Panel..... 2-2, 2-3
Related Documentation xxxi
Relay 5-6
Remote Management
  Firewall 8-1
Remote Management Limitations 20-3
Remote Management Setup..... 20-2
remote node 4-1
Remote Node
  Remote Node Setup 3-3
Remote Node Filter..... 4-10
Required fields..... 3-2
Restore Configuration..... 18-7
Return address 9-5
RIP.....5-4, 5-7, 4-8, 4-10
RoadRunner Support..... 1-3
Rule
  Summary Example 13-6
Rule Summary10-4, 13-1, 13-4, 13-6, 13-9, 13-10, 13-11, 13-14
Rules 10-1, 10-4
  Checklist 10-1
  Creating Custom..... 10-1
  Key Fields..... 10-2
  LAN to WAN 10-3
  Logic..... 10-1
  Predefined Services..... 10-7
  Source and Destination Addresses..... 10-11
  Summary 10-4
  Timeout..... 10-13

S

SA Monitor..... 24-1
Safety Instructions I
Saving the State 7-7
Schedule Sets
  Duration..... 21-2
Security Association 24-1
Security In General..... 7-12
Security Ramifications..... 10-2
Send Alerts When Attacked..... 13-7
Server..5-2, 6-2, 4-3, 6-5, 6-8, 6-10, 6-12, 6-13, 6-14, 6-15, 6-17, 6-18, 19-6
Service ..... vi, 10-2
Service Type 6-2, 4-2, 11-4, 26-2
setup a schedule 21-2
SMT..... 3-2
SMT Menus at a Glance..... 3-5, 3-7
SMTP Error Messages 9-6
Smurf..... 7-6
SNMP..... 16-1
  Configuring..... 16-3
    Community 16-3
    Trap..... 16-4
    Trusted Host..... 16-4
  Manager 16-2
  MIBs 16-3
SNMP (Simple Network Management Protocol) 1-2
SNMP (Simple Network Management Protocol)16-1
Source & Destination Addresses..... 10-11
Source Address..... 10-3, 10-10
SrcAdd 13-9
Stateful Inspection.....1-1, 7-1, 7-2, 7-7, 7-8
  Process 7-8
  ZyWALL..... 7-9
SUA (Single User Account) ..... *See* NAT
Subnet Mask .. 5-2, 5-3, 5-7, 6-2, 4-7, 4-9, 5-3, 10-13
Support Disk.....xxxi
Supporting Disk.....xxxi
SYN Flood..... 7-4, 7-5
SYN-ACK 7-5
Syslog 13-12
Syslog IP Address..... 17-7
System Information 17-1, 17-3, 17-4
System Maintenance. 17-1, 17-2, 17-3, 17-4, 17-5, 17-6, 17-7, 17-12, 17-13, 18-2, 18-5, 18-13, 18-15, 19-1, 19-2, 19-4, 19-6
System Status 17-1
System Timeout 20-4

T

TCP Maximum Incomplete..... 9-8, 9-9, 9-11, 9-11
TCP Security.....7-10
TCP/IP 5-1, 5-2, 5-5, 5-7, 4-7, 4-10, 7-3, 7-4, 15-7, 15-8, 15-10, 15-13, 15-17, 20-1
TCP/IP filter rule.....15-7
Teardrop 7-4
Telnet.....20-1
Telnet Configuration.....20-1
Telnet Under NAT 20-1
TFTP and FTP over WAN Will Not Work When….....18-4
TFTP and FTP Over WAN}.....20-3
TFTP File Transfer.....18-13
TFTP Restrictions 18-4, 20-3
Three-Way Handshake 7-5
Threshold Values.....9-7
Time and Date Setting 1-3, 19-5, 19-6
Time Zone.....19-7
Timeout..... 6-3, 6-5, 4-5, 10-13, 10-14, 10-15
Trace.....17-5
Traceroute 7-7
Troubleshooting 26-1
  Internet Access 26-3
  LAN Interface.....26-2
  WAN Interface.....26-2

U

UDP/ICMP Security 7-10
Unicast.....5-4
UNIX Syslog.....17-7
Upload Firmware.....18-10
Upper Layer Protocols 7-10, 7-11

V

Virtual Private Network 1-1
VT100 2-5

W

WAN DHCP 17-12, 17-13
WAN Setup.....4-3, 4-4, 26-2
WAN to LAN Rules 10-4
Web Configurator 7-2, 7-11, 8-2, 9-1, 10-2, 13-2
  HTML Help 9-2
  Login..... 9-1
  Password..... 9-1
www.zyxel.com.....vi

X

xDSL modem..... 1-4, 2-4, 2-5, 4-3, 26-2, 26-3
XMODEM protocol..... 18-2
XMODEM upload..... 3-8

Z

ZyNOS.....4-4, 17-3, 17-4, 18-1, 18-2
ZyNOS F/W Version 17-3, 17-4, 18-1
ZyWALL Firewall Application 7-3
ZyWALL Web Configurator..... 9-1
ZyXEL Limited Warranty
  Note vi
ZyXEL website.....vi
ZyXEL's Firewall
  Introduction..... 7-2